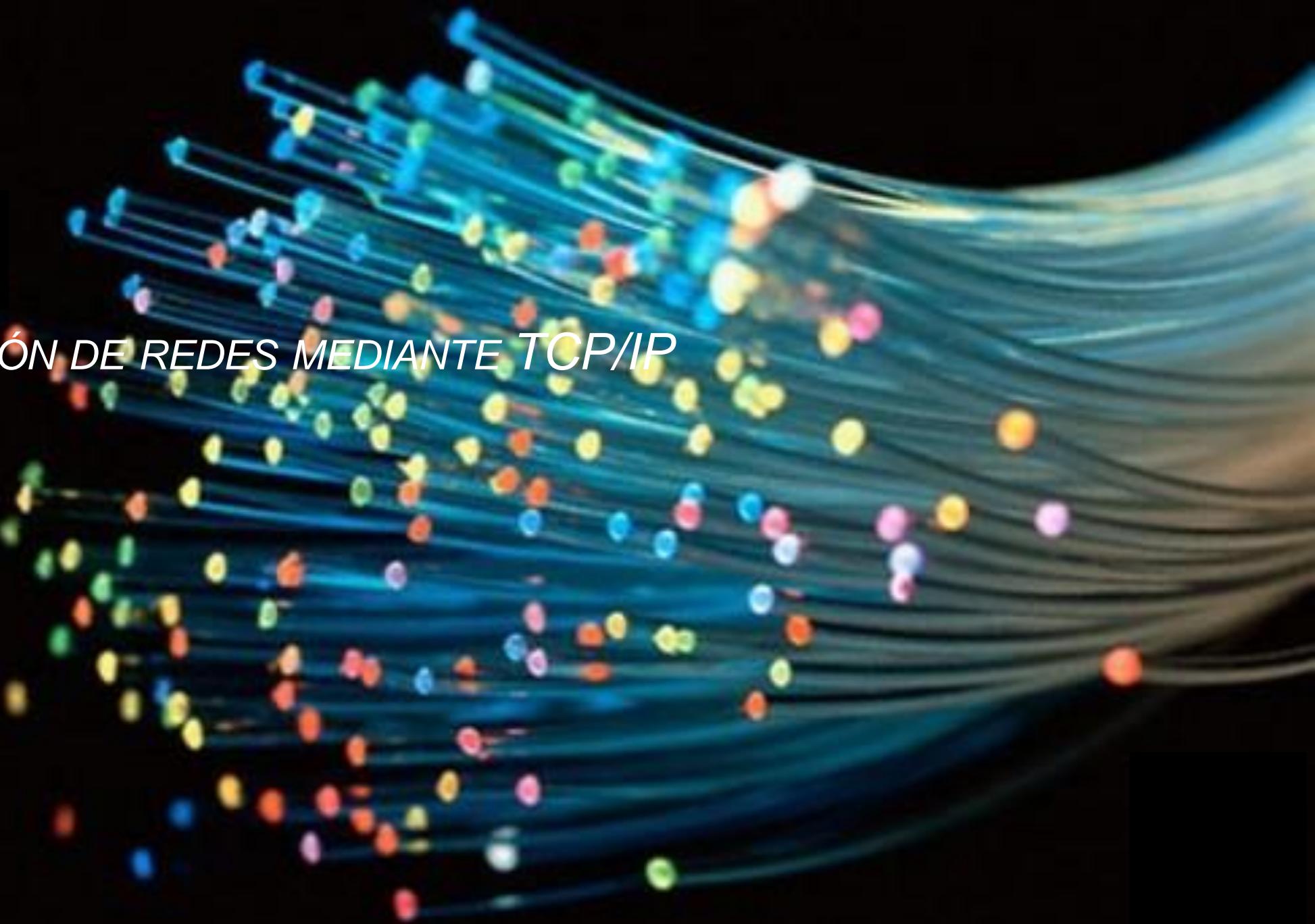
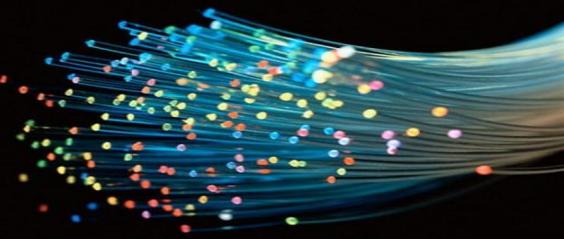


INTERCONEXIÓN DE REDES MEDIANTE TCP/IP





1. [Introducción](#)
2. [La arquitectura TCP/IP](#)
3. [La capa interfaz de red](#)
4. [La capa IP](#)
 1. [Direccionamiento IPv4](#)
 2. [Direccionamiento IPv6](#)
 3. [El datagrama IP](#)
 4. [El protocolo ICMP](#)
 5. [El encaminamiento](#)
 6. [Casos de estudio de encaminamiento](#)
5. [La capa de transporte](#)
6. [La capa de aplicación](#)

1. Introducción

La red Internet

Elementos de Internet

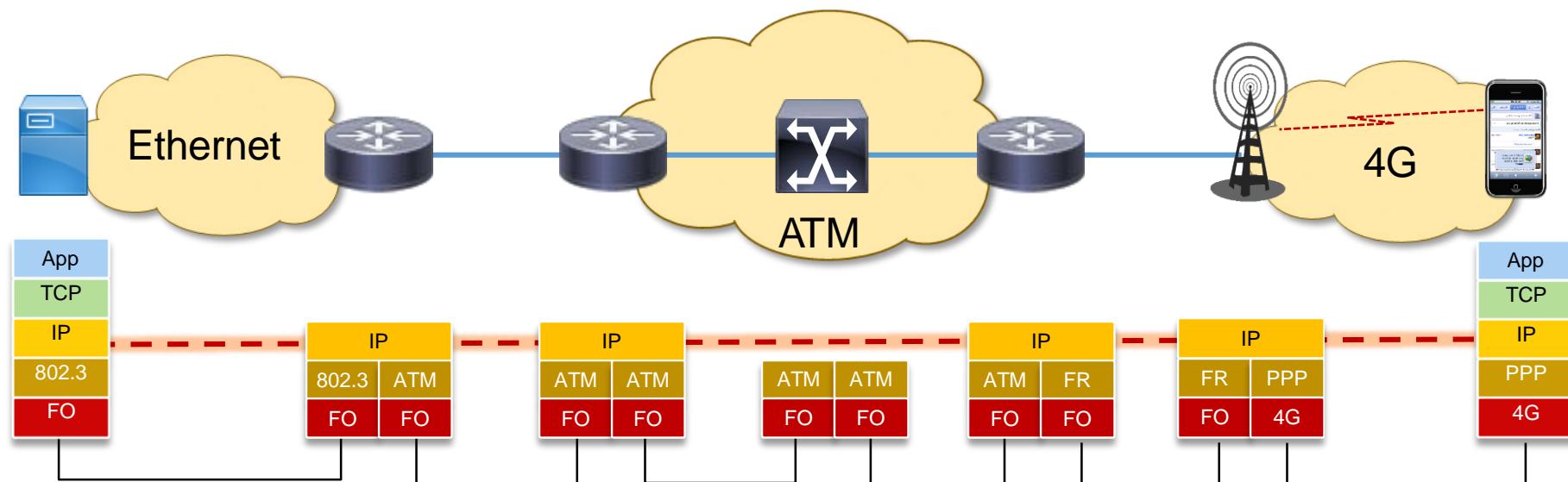
Dispositivos de Internet



La red Internet

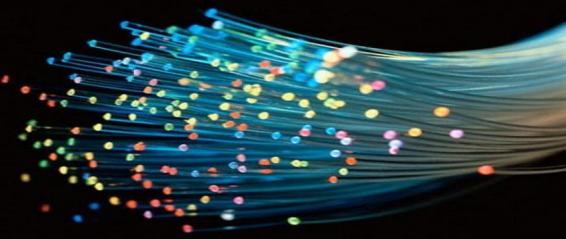


- La red Internet es un compendio de redes diferentes que comparten una pila de protocolos comunes que facilitan una conexión IP extremo-a-extremo

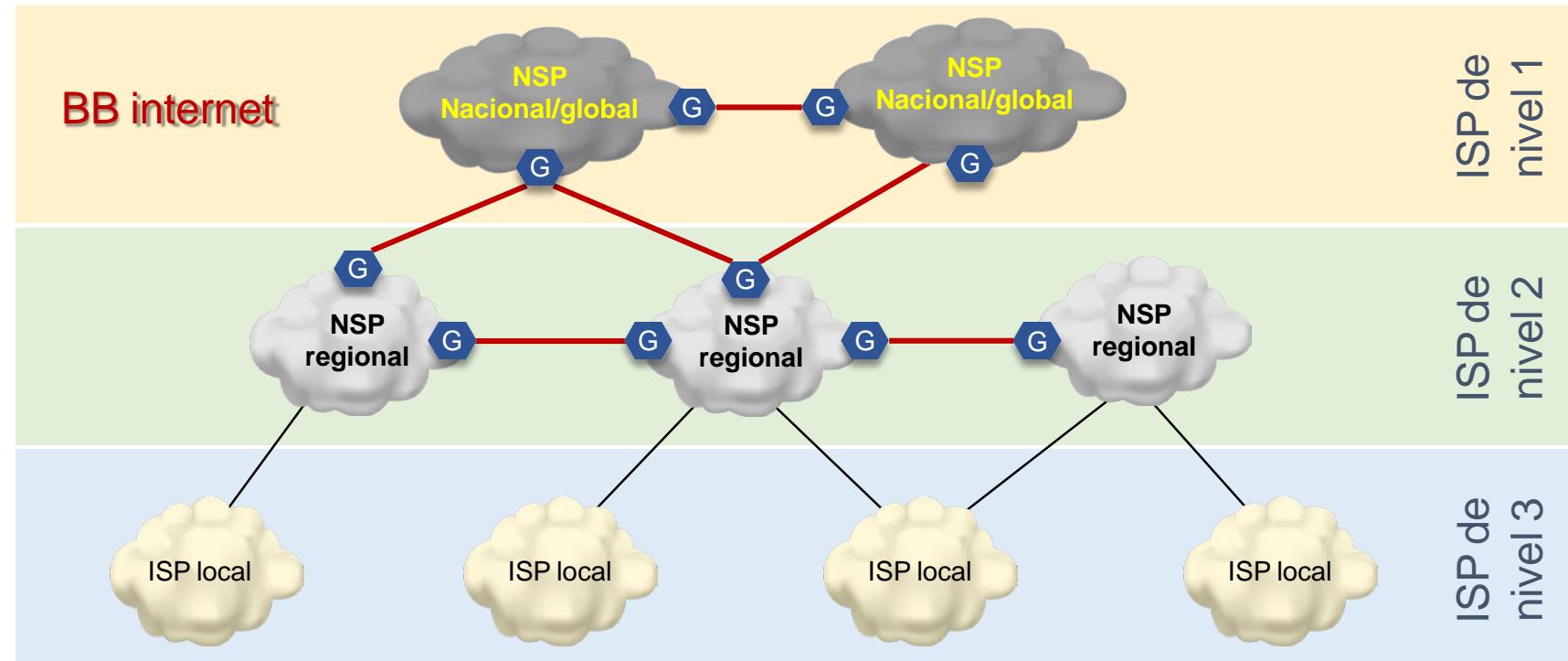


La red Internet

Estructura



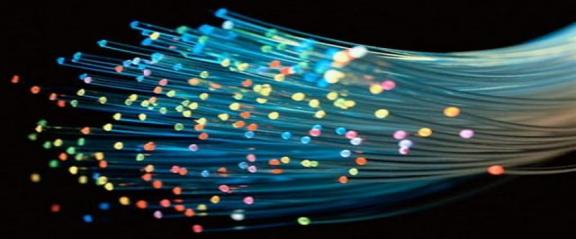
- A nivel de red, Internet puede definirse como un conjunto de redes conectadas entre sí por dispositivos conocidos como *gateways*



ISP: Internet Service Provider
NSP: Network Service Provider
G: Gateway
BB: Backbone

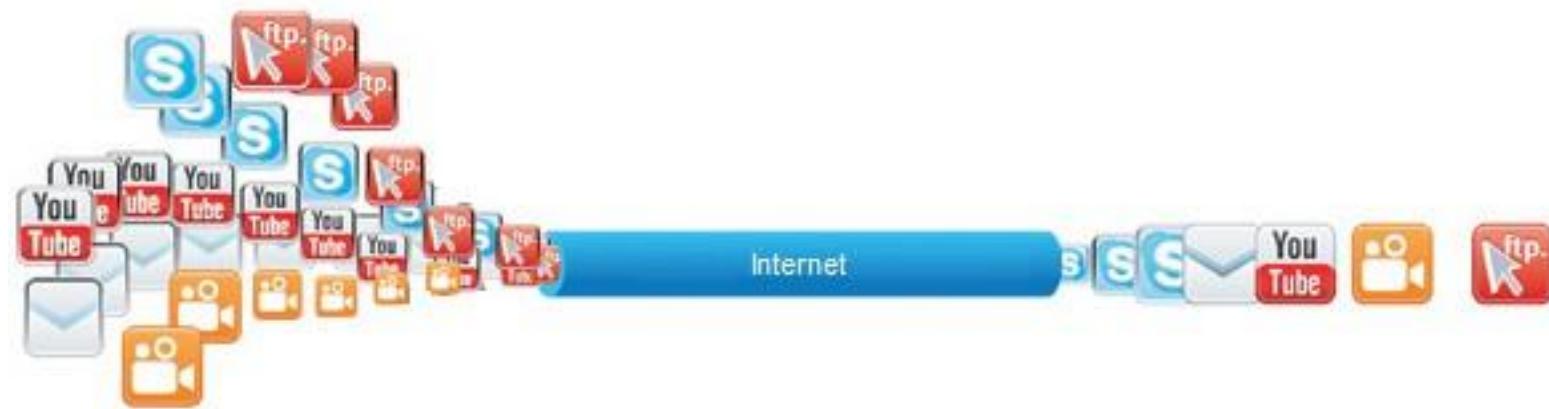
La red Internet

Servicio *Best effort*

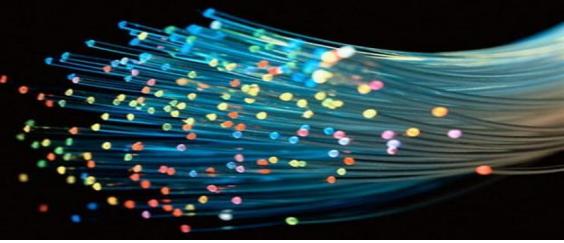


■ Las redes IP son redes de datagramas, no orientadas a conexión, con servicio *best effort*, es decir, no ofrece calidad de servicio

- Su desarrollo comenzó a finales de los 60, como un experimento de la agencia ARPA (*Advanced Research Projects Agency*), una agencia del Departamento de Defensa del gobierno de USA



Elementos de Internet



■ Infraestructura:

- líneas, conexiones, nodos, ...

■ Dispositivos:

- Host, Routers, Firewalls.

■ Direcciones (IP) y nombres de dominio.

■ Protocolos:

- de red (IP), de transporte (TCP, UDP).

■ Aplicaciones:

- telnet, rlogin, ftp, mail, www, ...

Dispositivos de Internet



HOSTS

- Un único interfaz de red. Una sola dirección IP



MULTIHOMED HOST

- Más de una interfaz de red. Varias direcciones IP. Una por cada interfaz



ROUTERS o GATEWAYS

- Encaminar Datagramas
- Varios interfaces de red
- Unen redes o subredes



FIREWALS o CORTAFUEGOS

- Varios interfaces de red
- Aíslan redes o subredes

2. La arquitectura TCP/IP

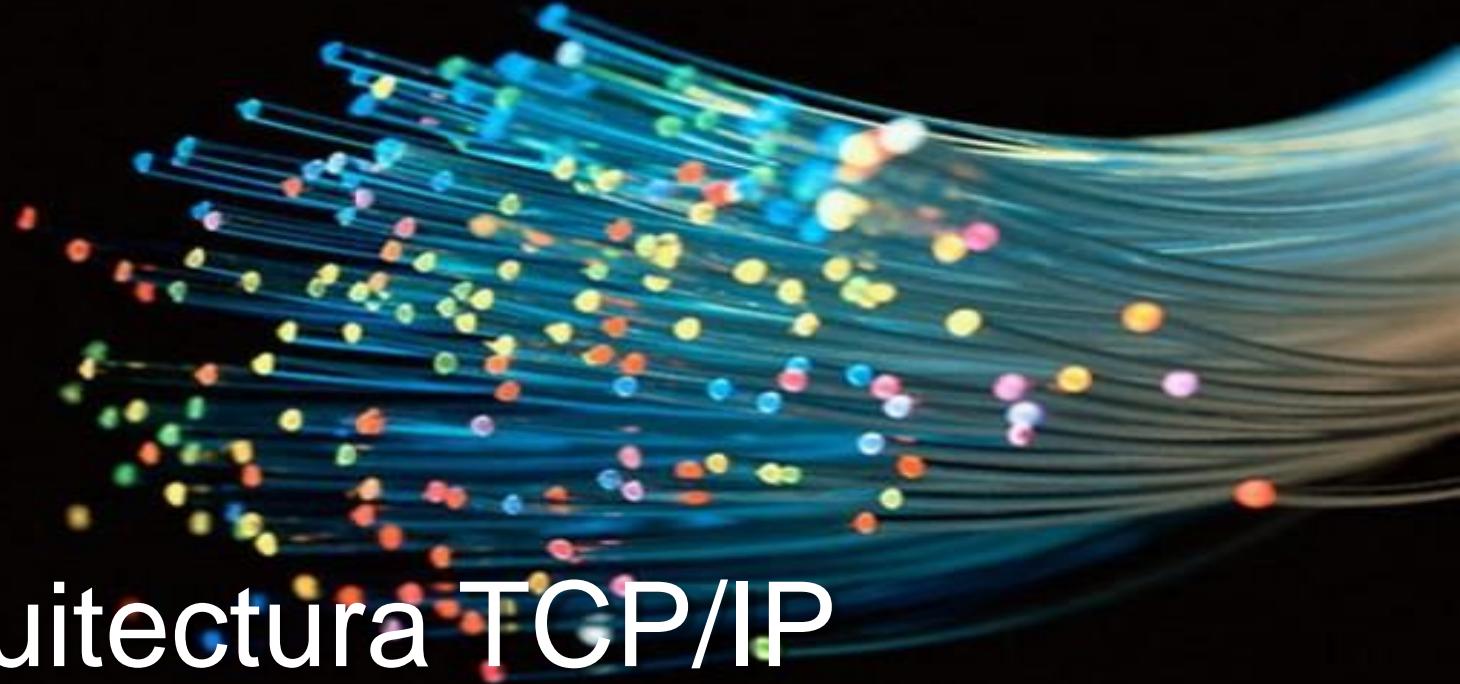
Introducción a TCP/IP

Arquitectura TCP/IP vs OSI

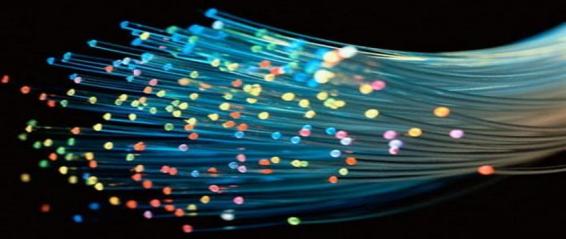
Arquitectura TCP/IP. Encapsulación

Capas propias del host: Aplicación y transporte

Capas de red: IP e interfaz de red

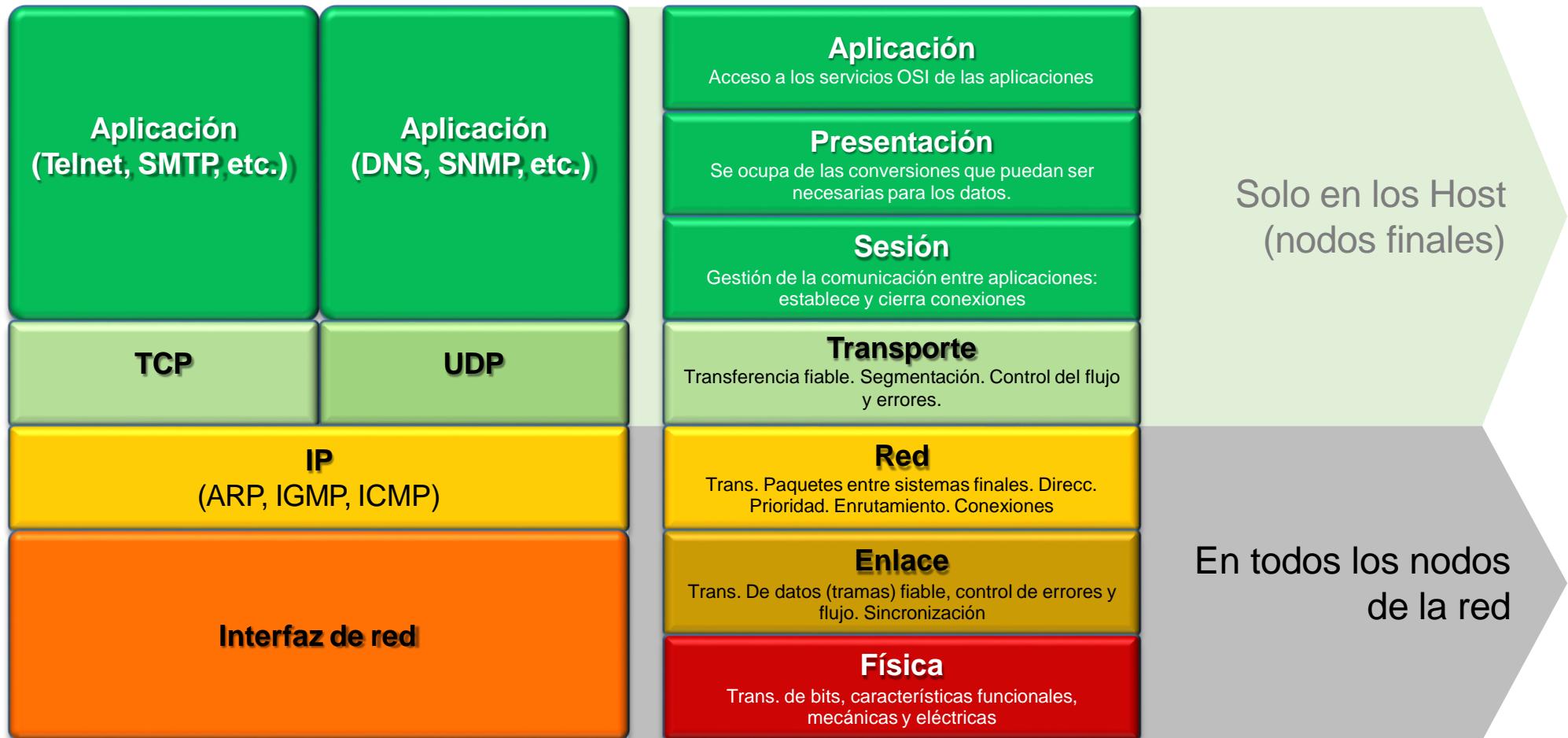


Introducción a TCP/IP



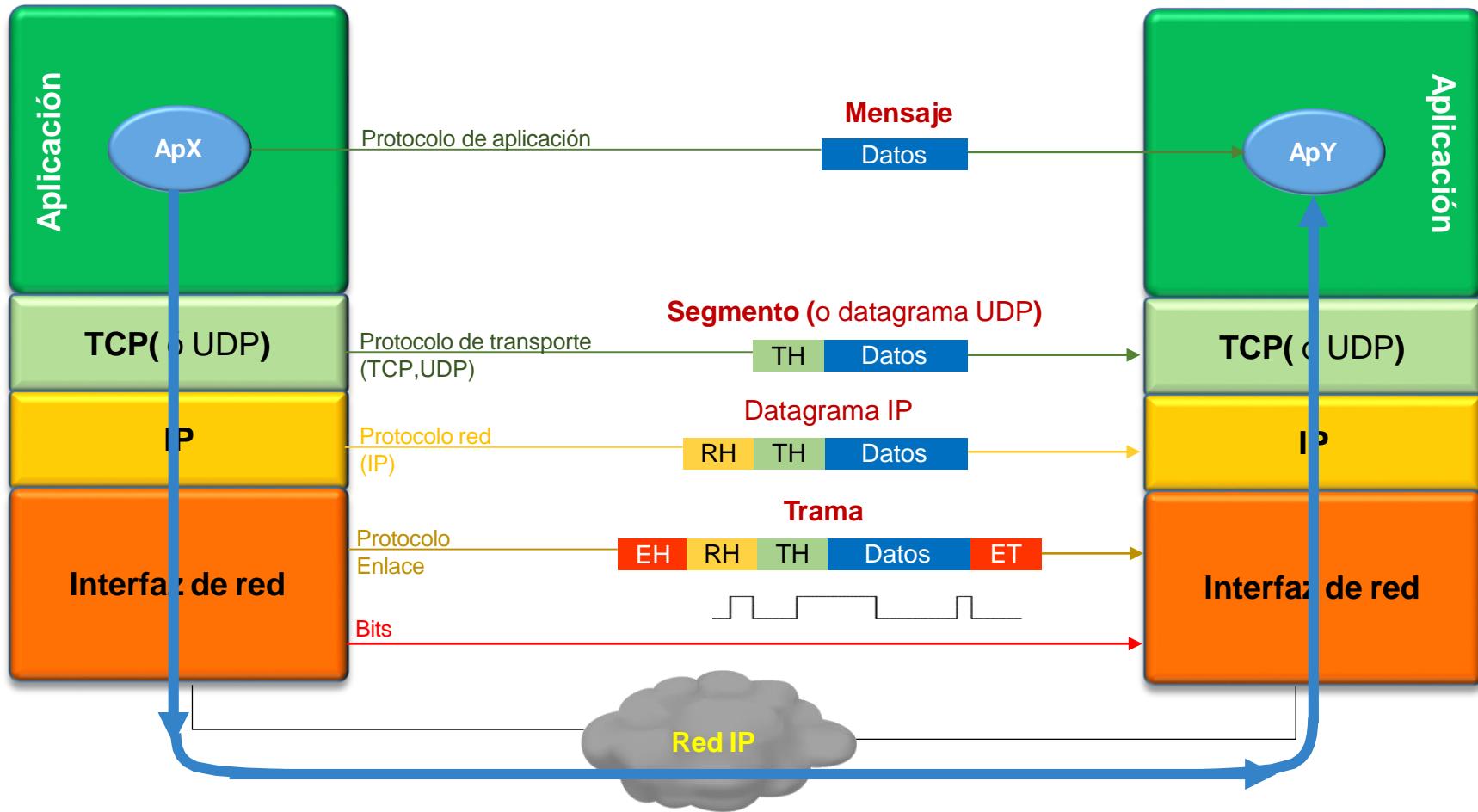
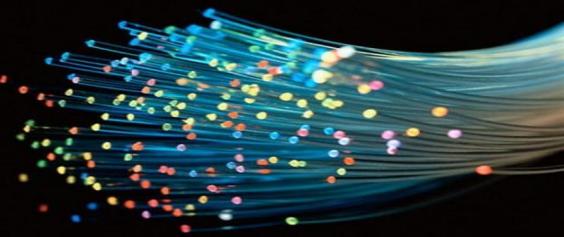
- TCP/IP constituye el armazón sobre el que se asienta Internet
- El conjunto de protocolos TCP/IP permite la comunicación entre diferentes máquinas, independientemente de la tecnología:
 - Diferentes sistemas operativos
 - Diferentes tipos de máquinas
 - Diferentes tipos de red
- **TCP/IP es un auténtico sistema abierto:** Los protocolos y sus implementaciones están disponibles públicamente

Arquitectura TCP/IP vs OSI



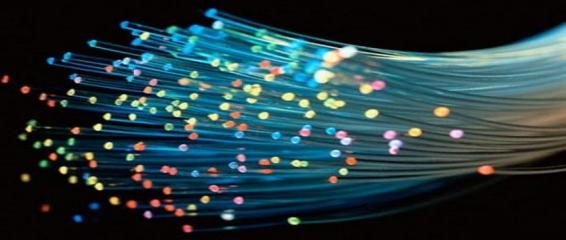
Arquitectura TCP/IP

Encapsulación



Arquitectura TCP/IP

Capas propias del host



Aplicación

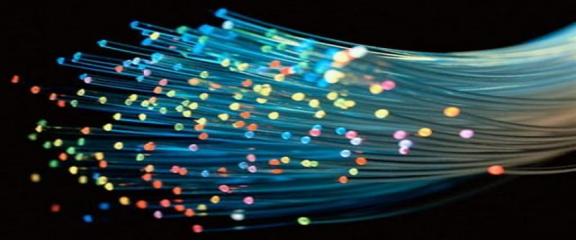
- **Interfaz con los servicios finales.** Contiene toda la lógica necesaria para posibilitar las distintas aplicaciones de usuario
- Las aplicaciones acceden a la capa de transporte por los **puertos** asignados
- Protocolos: FTP, Telnet, WWW, DNS,

Transporte (TCP, UDP)

- **Transferencia entre procesos de aplicación extremo-extremo**
- Identificación de procesos mediante Puertos
- **TCP** (*Transport Control Protocol*): orientado a conexión y complejo
- **UDP** (*User Datagram Protocol*): No orientado a conexión y mas sencillo

Arquitectura TCP/IP

Capas de red



Internet

- **Gestiona el movimiento de paquetes por la red**
- Transferencia entre máquinas origen y destino
- Identificación mediante Direcciones IP
- No fiable y no orientado a conexión
- Encaminamiento y Fragmentación
- Comunica errores (con ICMP y SNMP)

Interfaz de red

- **Proporciona los drivers que interactúan con los componentes hardware para adaptar y configurar el nivel físico**
- Funciones de nivel físico y de enlace

3. La capa interfaz de red

La interfaz de red

IP sobre Ethernet

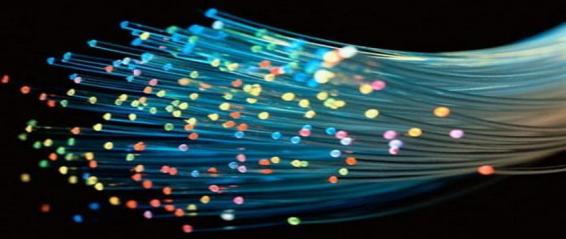
El problema de la resolución de las direcciones IP

Resolución de las direcciones IP

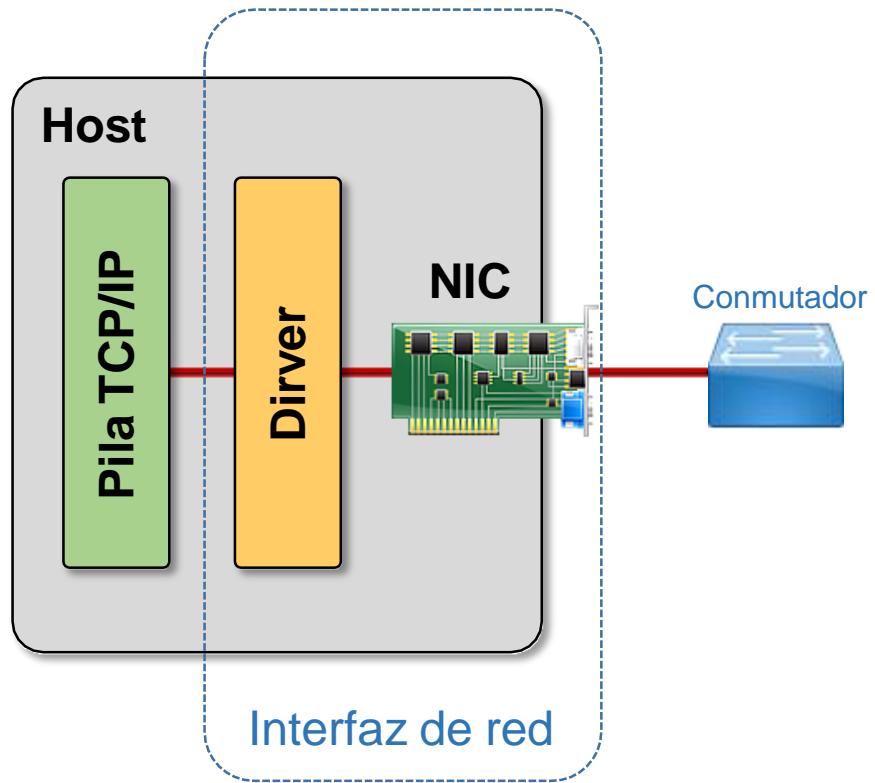
El protocolo ARP



La interfaz de red

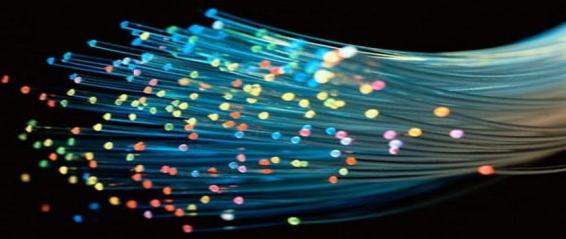


- El uso de IP hace necesario implantar niveles intermedios entre el propio IP y las subredes sobre las que descansa.
 - IP es único. Redes hay muchas.
- La **Interfaz de red** es un módulo periférico (placa de red) que actúa como interfaz de conexión entre un computador (host) y la red
- Cada **interfaz de red tiene una dirección IP** única



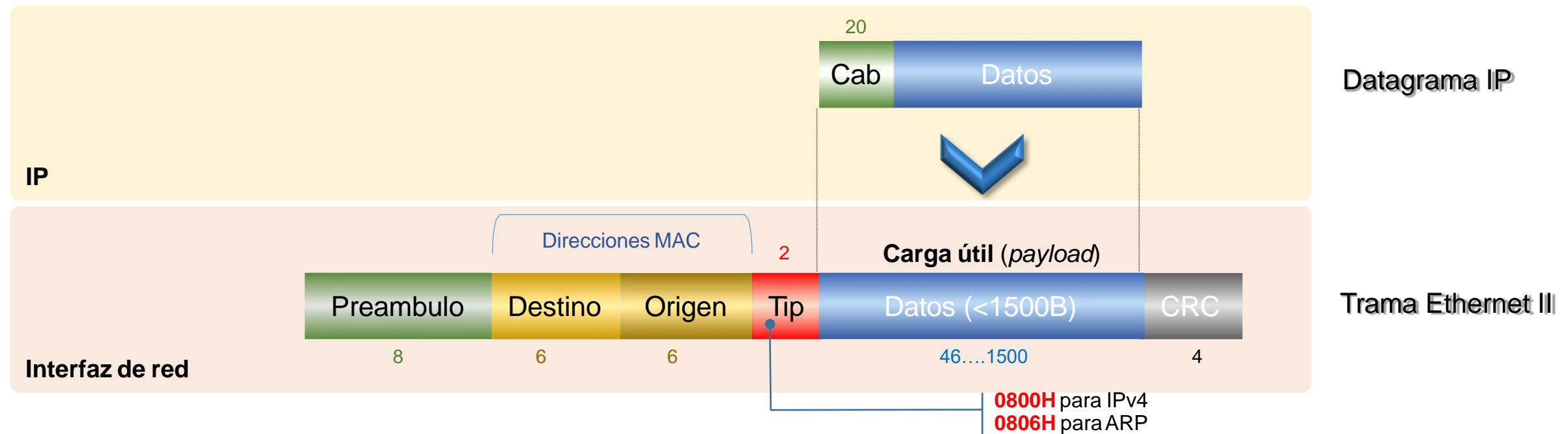
Interfaz de red

Ejemplo con Ethernet

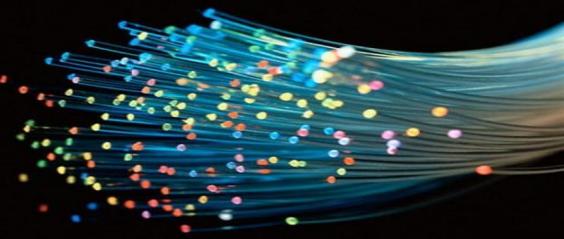


IP sobre Ethernet

- 1) Se genera el datagrama IP con su correspondiente cabecera
- 2) Se construye la trama Ethernet:



IP sobre Ethernet

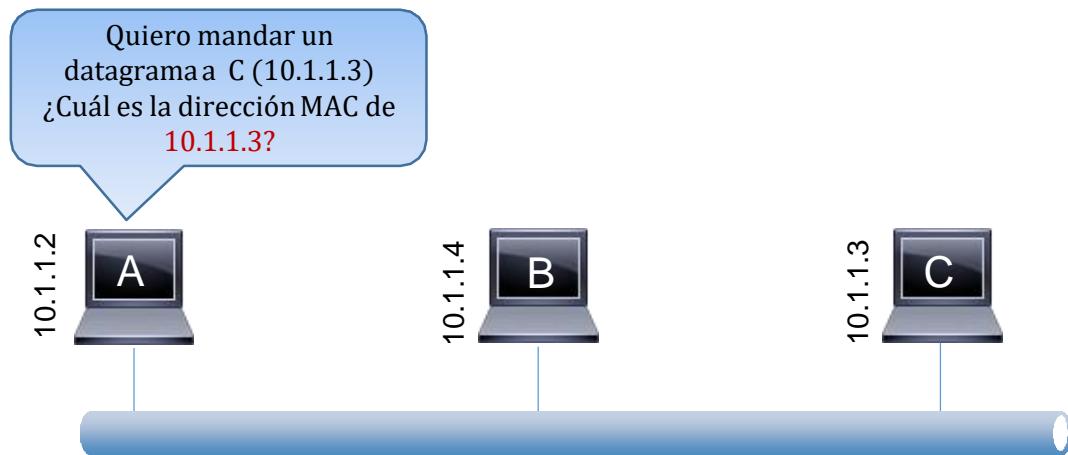


- Las tarjetas de red Ethernet tienen una dirección MAC única alojada en el HW
 - Esta dirección se utiliza en el campo de dirección Origen/Destino de la trama Ethernet.
- El campo Longitud/Tipo de la trama MAC Ethernet muestra la longitud de la trama o el tipo de protocolo que transporta la trama:
 - 0800H para IP
 - 0806H para ARP
- Una máquina “escuchando la red” y ejecutando una aplicación TCP/IP comprobará si el campo L/T es 0800H o 0806H.
- Una estación ejecutando otro protocolo dará las tramas anteriores como inválidas

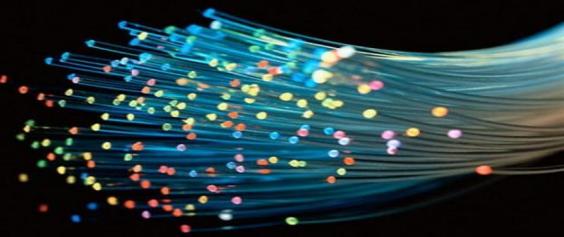
El problema de la resolución de las direcciones IP

Las direcciones IP son abstracciones proporcionadas por la capa IP.

Debido a que el hardware de red física (Ethernet, en este caso) de un sistema no sabe cómo localizar un ordenador por su dirección IP, esta debe ser **traducida a una dirección MAC equivalente** antes de enviar una trama.



Resolución de las direcciones IP

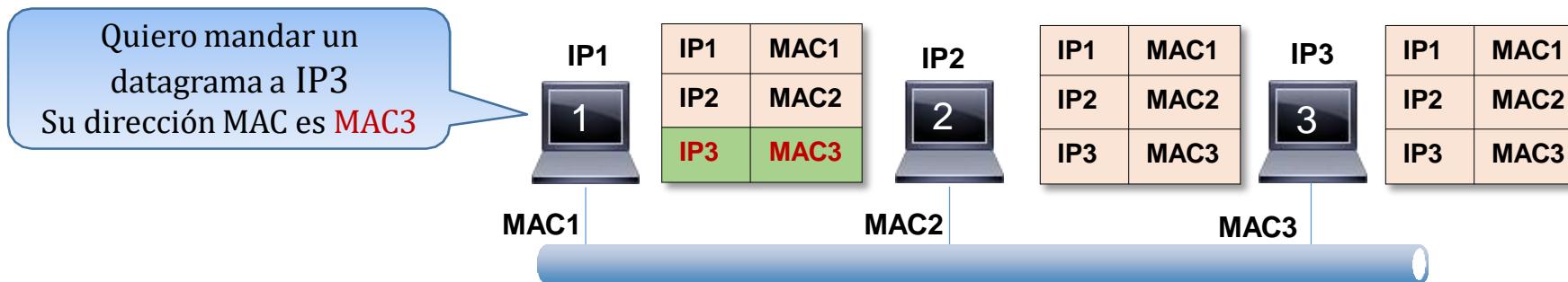


Mediante tablas estáticas

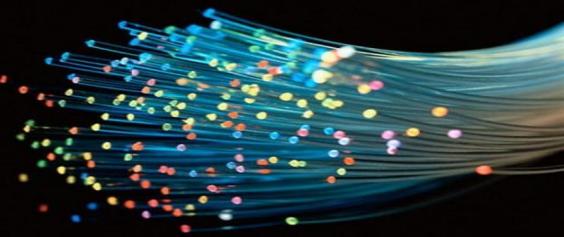
■ **Problema:** Dada una dirección IP, obtener la dirección MAC correspondiente: $\text{dir}_{\text{MAC}} = f(\text{dir}_{\text{IP}})$.

■ **Solución estática:**

- Tablas estáticas (una en cada host) mantenidas manualmente
- Principal inconveniente: necesidad de actualizar las tablas en todos los nodos de la red cada vez que se produce alguna modificación en la tabla de direcciones.



Resolución de las direcciones IP

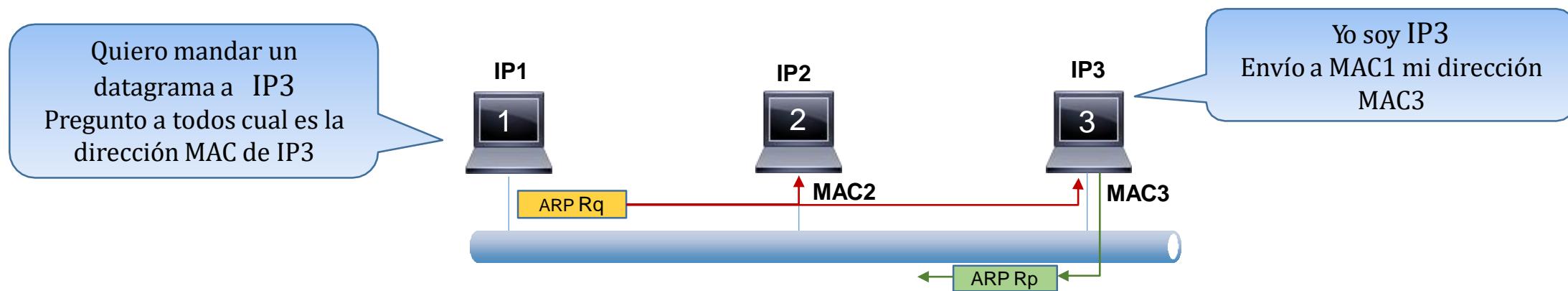


Mediante asociación dinámica

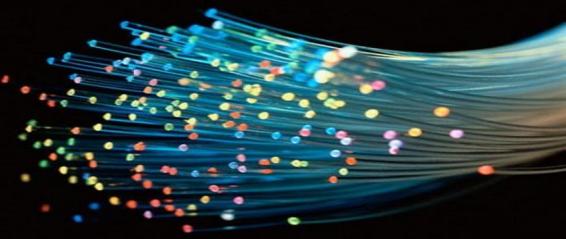
■ **Problema:** Dada una dirección IP, obtener la dirección MAC correspondiente:
 $\text{dir}_{\text{MAC}} = f(\text{dir}_{\text{IP}})$.

■ **Solución dinámica:**

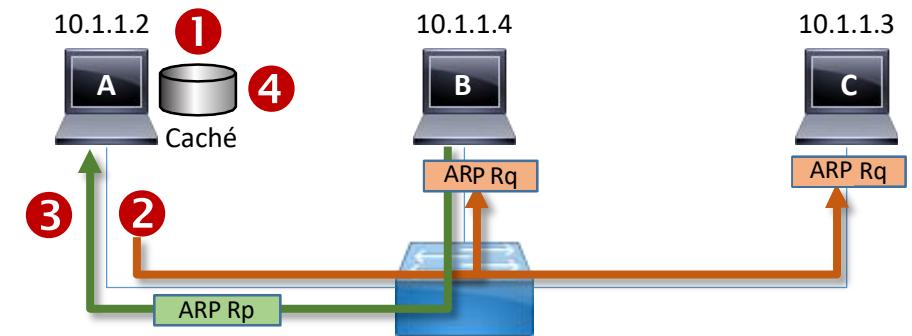
- Se construye un paquete (**ARP request**) en el que se escribe lo que sabemos y lo que queremos saber y se manda a la dirección MAC FF:FF:FF:FF:FF:FF (broadcast)
- Sólo responde el que reconozca su dirección IP en el *target*, y lo hace con un paquete **ARP response**
- Las direcciones resueltas vía ARP se mantienen un cierto tiempo en caché, en previsión de usos futuros



El protocolo ARP

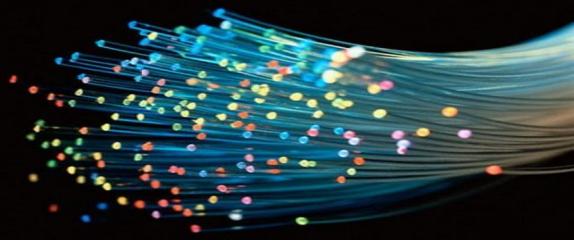


- Como se ha visto, en una LAN hace falta un mecanismo que permita descubrir a qué dirección MAC corresponde la dirección IP del paquete a entregar
- **El protocolo ARP** es ese mecanismo, permitiendo la configuración automática de correspondencias **dirección MAC-dirección IP**
- **Funcionamiento:**
 - 1) El host A busca en su propia caché de ARP local una dirección de Ethernet coincidente para la IP del host B (10.1.1.4)
 - 2) Si el host A no encuentra ninguna asignación, difunde una trama **ARP request** preguntando por la dirección Ethernet cuya dirección IP es B.
 - 3) Sólo "B" contestará, porque la dirección IP especificada en la solicitud ARP coincide con su propia dirección, enviando a "A" un paquete ARP indicando su dirección IP y su dirección Ethernet.
 - 4) Las direcciones resueltas vía ARP se mantienen un cierto tiempo en la caché ARP, en previsión de usos futuros.

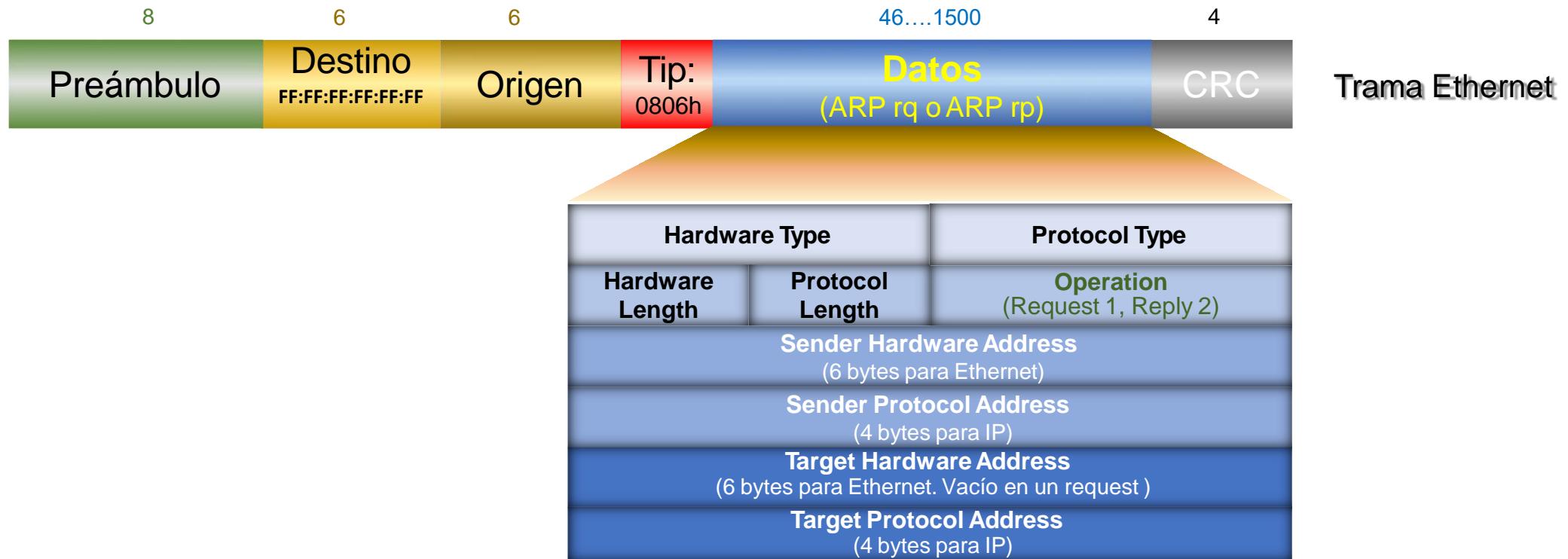


El protocolo ARP

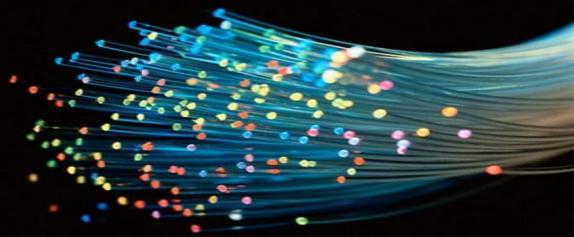
Formato



- ARP es un protocolo de nivel de red muy sencillo en el que solamente existen dos PDUs (*Packet data unit*): *ARP Request* y *ARP Reply*.



La caché de ARP

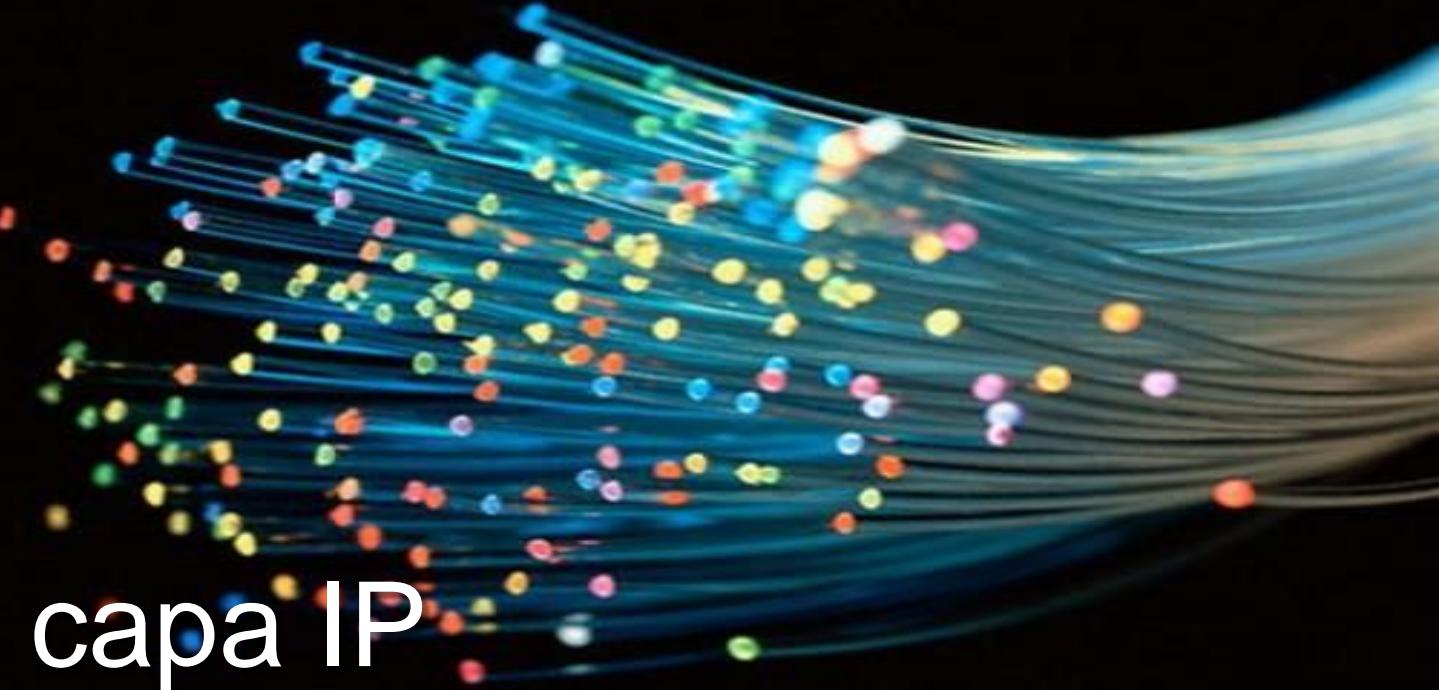


- Para disminuir el número de difusiones, ARP mantiene una tabla caché de asignaciones de direcciones
 - Se puede ver la caché de ARP con el comando **arp** del sistema

Administrador: Símbolo del sistema

```
C:\>arp -a
Interfaz: 192.168.1.36 --- 0x4
          Dirección de Internet      Dirección física     Tipo
 10.155.175.130      00-03-91-7d-2e-ca  dinámico
 192.168.1.1        a0-ec-80-27-b0-a6  dinámico
 192.168.1.35        f0-f6-1c-63-0b-ce  dinámico
 192.168.1.40        88-9b-39-31-c9-df  dinámico
 192.168.1.255       ff-ff-ff-ff-ff-ff  estático
 224.0.0.2          01-00-5e-00-00-02  estático
 224.0.0.22         01-00-5e-00-00-16  estático
 224.0.0.251        01-00-5e-00-00-fb  estático
 224.0.0.252        01-00-5e-00-00-fc  estático
 224.1.1.1          01-00-5e-01-01-01  estático
 239.0.0.90          01-00-5e-00-00-5a  estático
 239.0.2.2          01-00-5e-00-02-02  estático
 239.0.2.30         01-00-5e-00-02-1e  estático
 239.0.2.129        01-00-5e-00-02-81  estático
 239.0.2.155        01-00-5e-00-02-9b  estático
 239.255.255.250    01-00-5e-7f-ff-fa  estático
 255.255.255.255   ff-ff-ff-ff-ff-ff  estático

C:\>
```



4. La capa IP

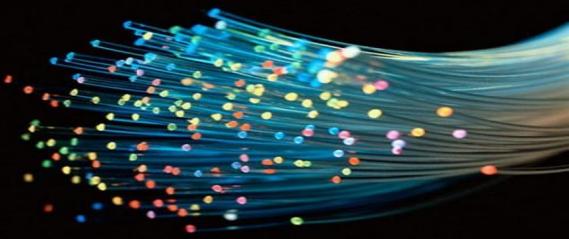
- 4.1. Direccionamiento IPv4
- 4.2. Direccionamiento IPv6
- 4.3. El datagrama IP
- 4.4. El encaminamiento
- 5.5. Casos de estudio de encaminamiento

4.1. Direccionamiento IPv4

El esquema de direccionamiento IP
Direccionamiento IP con clase
Direccionamiento IP sin clase
Subredes. Caso de estudio
El subneteo de tamaño variable (VLSM)
Agregación de rutas
Superredes. Caso de estudio
Direcciones IP privadas
NAT (*Network Address Translation*)



El esquema de direccionamiento IP



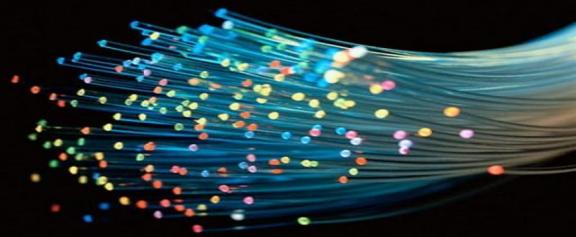
Para proporcionar un direccionamiento **uniforme** en Internet, el estándar IP define un esquema de direccionamiento **abstracto** que asigna a cada interfaz de red una dirección de protocolo IP **única**.

En concreto, una dirección de Internet (**IPv4**) es un número binario de 32 bits **único**, entre 4.000 millones de direcciones posibles.

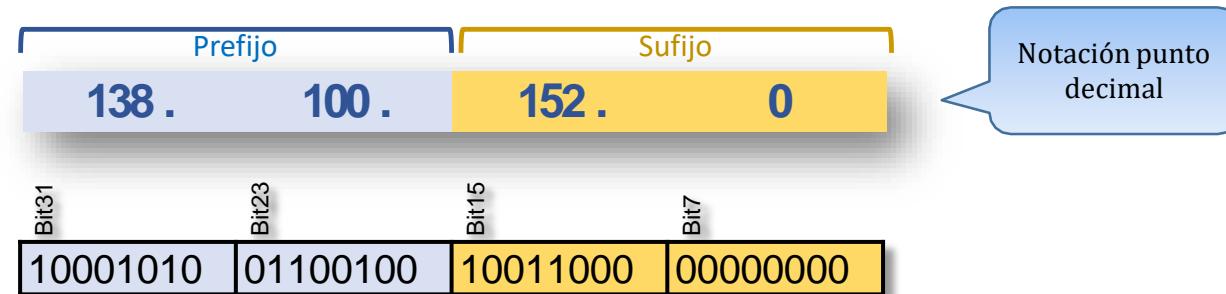
- El esquema de direccionamiento IP es independiente de las direcciones MAC subyacentes
- En los paquetes IP, los campos dirección origen y destino situados en la cabecera IP contienen cada uno una dirección internet global de 32 bits

El esquema de direccionamiento IP

Características



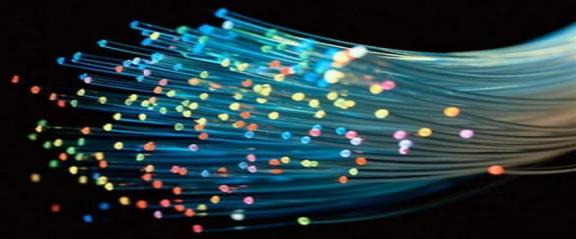
- La dirección IP es un número de 32 bits, dividido jerárquicamente en un **prefijo** y un **sufijo**:
 - El **prefijo** identifica la red a la que está conectado el ordenador y no puede haber 2 redes con el mismo prefijo
 - El **sufijo** identifica al host dentro de esa red, de tal forma que no puede haber dos equipos de la misma red que tengan el mismo sufijo
 - Las direcciones IP se suelen representar mediante cuatro números decimales separados por puntos (**notación punto decimal**)



IPv4 permite $2^{32} = 4.294.967.296$ direcciones
Población mundial en 2015 = 7.376.471.981 millones

Direccionamiento IP con clase

Clases principales



- En 1981, los diseñadores dividieron el espacio de direcciones IP en tres formatos **fijos** de dirección (**clases**), donde cada clase tiene un prefijo y sufijo de diferente tamaño para adaptarse a las diferentes dimensiones de red
 - Este tipo de direccionamiento recibió el nombre de **classful addressing**

Clase A

10 . 1 . 1 . 3

$2^7=128$ Redes; $2^{24}=16.777.216$ Host

Bit3	Bit2	Bit1	Bit7
0	00001010	00000001	00000001

Clase B

172 . 4 . 3 . 59

$2^{14}=16.384$ Redes; $2^{16}=65.536$ Host

Bit3	Bit2	Bit1	Bit7
10	101100	00000100	00000011

Clase C

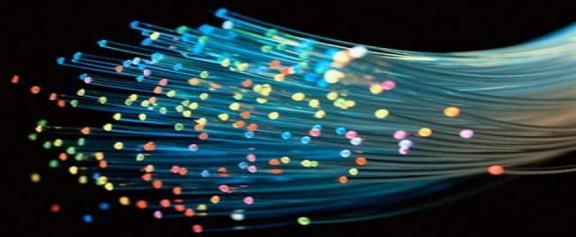
192 . 168 . 192 . 1

$2^{21}=2.097.152$ Redes; 256 Host

Bit3	Bit2	Bit1	Bit7
110	00000	10101000	11000000

Direccionamiento IP con clase

Clases especiales



- La Clase D está reservada para las direcciones *multicast* (multidestino)
 - Cada dirección multicast identifica un grupo de computadores
 - Aplicaciones: videoconferencia; aprendizaje a distancia; distribución de software, de video, etc.

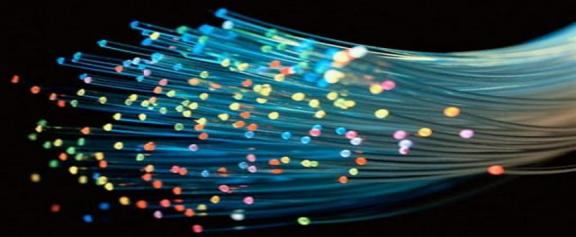


- La Clase E se utiliza para propósitos experimentales solamente.
 - IETF ha reservado estas direcciones para su propia investigación. Por lo tanto, las direcciones de Clase E no pueden ser utilizadas en Internet.



Direccionamiento IP con clase

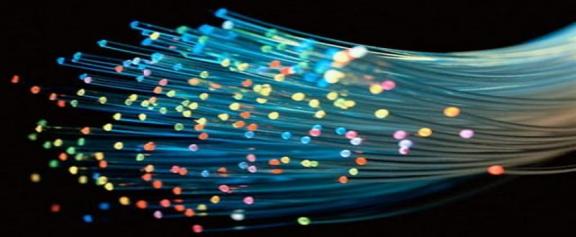
Rangos de direcciones. Clase A



- Esta clase de direcciones permite tener muchos sistemas conectados en una única subred. Es apropiada para una gran compañía
- El primer bit (el más significativo) va a 0
- Restricciones
 - 0.0.0.0 se dedica para **dirección de encaminamiento por defecto**
 - El rango de 127.0.0.0 a 127.255.255.255 está reservado para **direcciones de loopback** o de circuito cerrado (a uno mismo)
 - El rango 10.0.0.0 a 10.255.255.255 es para uso privado

Direccionamiento IP con clase

Rangos de direcciones. Clase B

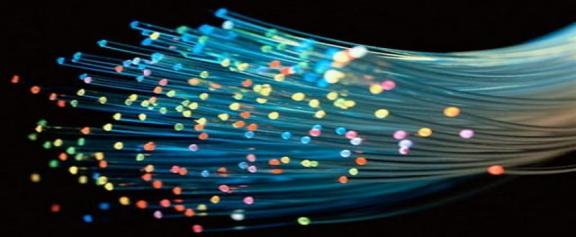


Desde					Hasta					Redes	Host
128 . 0 . 0 . 0					191 . 255 . 255 . 255					16.384	65.534
10000000 00000000 00000000 00000000					10111111 11111111 11111111 11111111						

- La clase B se utiliza para las redes de tamaño mediano. Un buen ejemplo es un campus grande de la universidad
- Los dos bits de mayor peso son siempre **10**
- Restricciones
 - Las siguientes direcciones son para uso privado
 - ✓ 169.254.0.0/16
 - ✓ 172.16.0.0/12

Direccionamiento IP con clase

Rangos de direcciones. Clase C

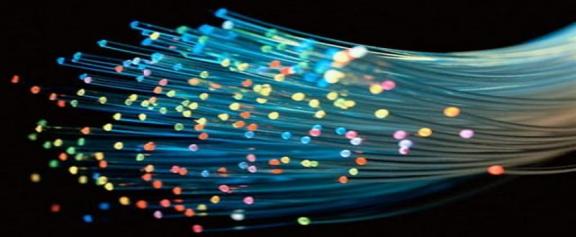


Desde				Hasta				Redes	Host
192 . 0 . 0 . 0				223 . 255 . 255 . 255				2.097.152	254
11000000 00000000 00000000 00000000				11011111 11111111 11111111 11111111					

- Las direcciones de la clase C se utilizan comúnmente para las compañías pequeñas a medianas.
- Los dos bits de mayor peso son siempre **110**
- Entre las numerosas restricciones destacamos:
 - 192.0.0.0/24 reservada para el Registro de Direcciones IPv4 de IANA
 - 198.18.0.0/15 que se utiliza para la prueba de las comunicaciones entre dos subredes independientes
 - El rango 192.168.0.0/16 es para uso privado

Direccionamiento IP con clase

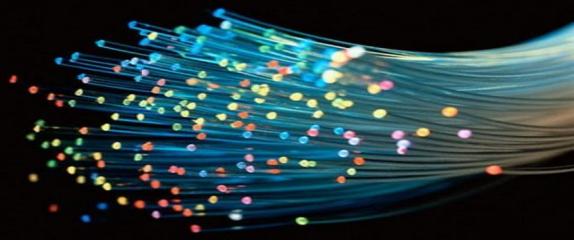
Rangos de direcciones. Resumen



	Desde	Hasta	Redes	Host
Clase: A	1 . 0 . 0 . 0	127 . 255 . 255 . 255	126	16.777.214
Clase: B	128 . 0 . 0 . 0	191 . 255 . 255	16.384	65.534
Clase: C	192 . 0 . 0 . 0	223 . 255 . 255 . 255	2.097.152	254
Clase: D	224 . 0 . 0 . 0	239 . 255 . 255 . 255	NA	NA
Clase: E	240 . 0 . 0 . 0	247 . 255 . 255 . 255	NA	NA

Direccionamiento IP sin clase

CIDR



Como consecuencia del crecimiento exponencial de Internet, y el agotamiento del espacio de direcciones, se vio que el direccionamiento con clases (**classfull**) era poco flexible y eficiente

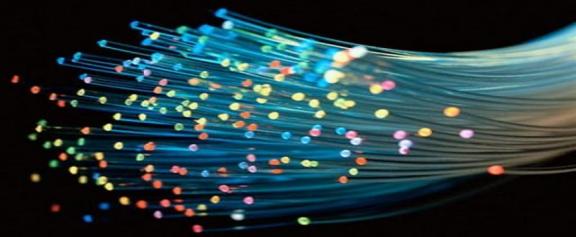


La respuesta a este reto, en los 90, fue la invención de la Subred y el desarrollo del **direccionamiento sin clases (CIDR)**, que se fundamenta en:

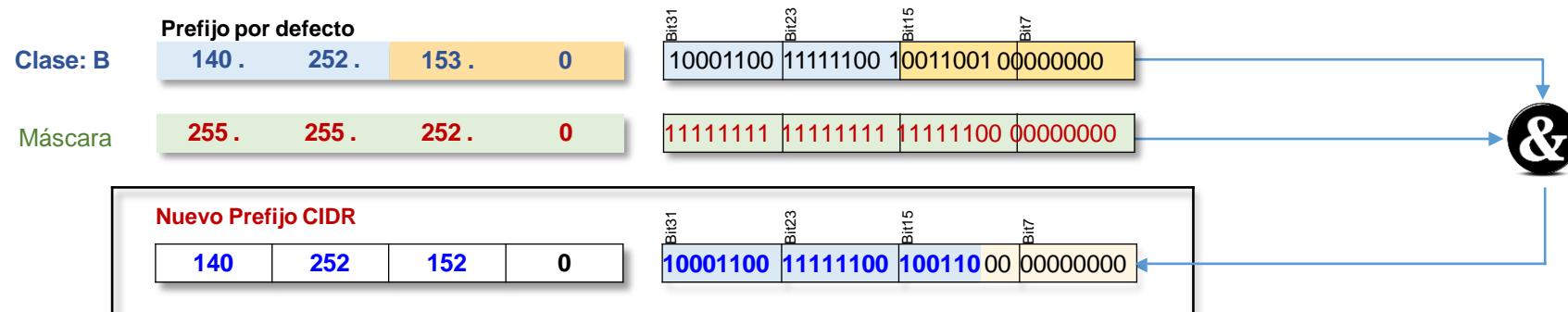
- a) Eliminar el concepto tradicional de la **Clase A, Clase B y Clase C**, y
- b) Sustituirlo por el concepto de **prefijo de red**, que permite definir bloques de direcciones de cualquier tamaño. Así, los routers utilizarían el **prefijo de red**, en lugar de los 3 primeros bits de la dirección IP, para determinar el punto de división entre el número de red y el número de host

Direccionamiento IP sin clase

Concepto de máscara

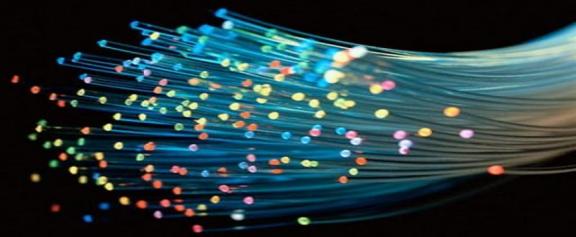


- El direccionamiento CIDR requiere, en hosts y routers, un dato adicional: un valor (o parámetro) que especifica el límite exacto entre el prefijo de red y el sufijo
- Ese parámetro, de 32 bits, es conocido como **máscara de dirección**
 - Si un bit de la máscara está a **1**, el bit correspondiente de la dirección se interpreta como bit de red
 - Si un bit de la máscara está a **0**, el bit correspondiente de la dirección se interpreta como bit de host



Direccionamiento IP sin clase

Notación CIDR



- Con el fin de especificar e interpretar los valores de máscara, la tradicional notación decimal con puntos de la dirección se amplió, incorporando a la misma un número que expresa la máscara (**notación CIDR**)
 - La máscara se indica seguida de una barra y un número decimal que especifica el número de "1"contiguos, empezado por la izquierda de la máscara

ddd.ddd.ddd.ddd / m

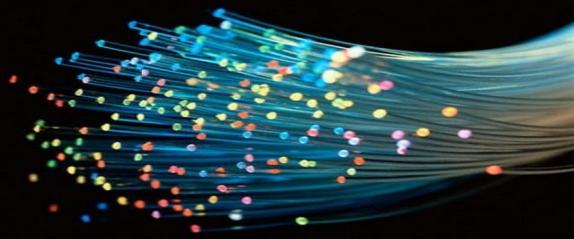
donde ddd es el valor decimal de un octeto de la dirección y **m** es el número de unos de la máscara.

192.5.48.69 / 26

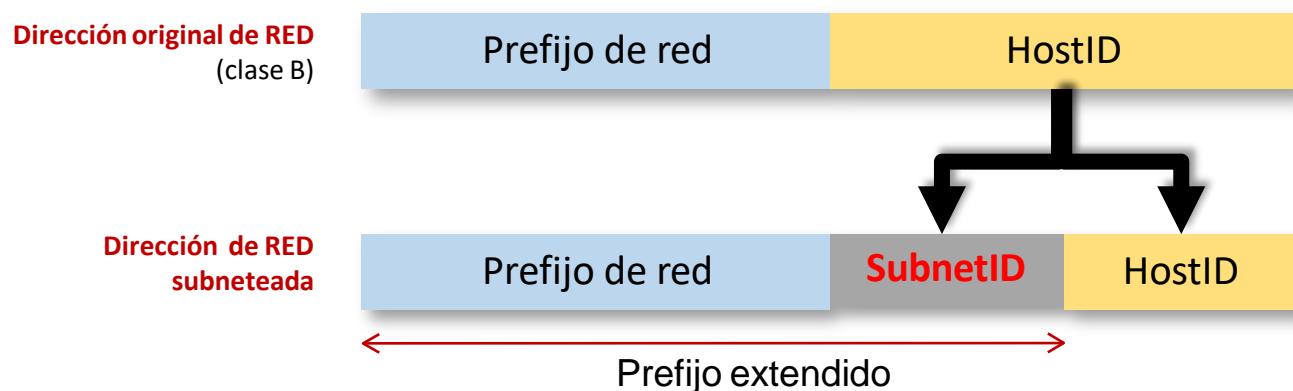
Se especifica una máscara de 26 bits, esto es:
11111111. 11111111.
11111111.11000000

Direccionamiento IP sin clase

Subredes

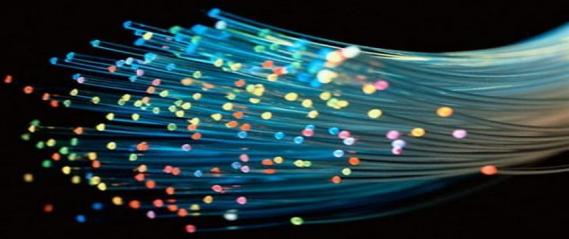


- Una red física (A,B o C) se puede dividir en múltiples redes más pequeñas (**subredes**) tomando bits de la parte de HOST de la dirección
 - Los routers constituyen los límites entre las subredes
 - Para crear subredes se define una **máscara** en la que están a 1 los bits de la red-subred (prefijo extendido), y a 0 los del host
 - Las subredes mejoran la asignación de direcciones y el encaminamiento



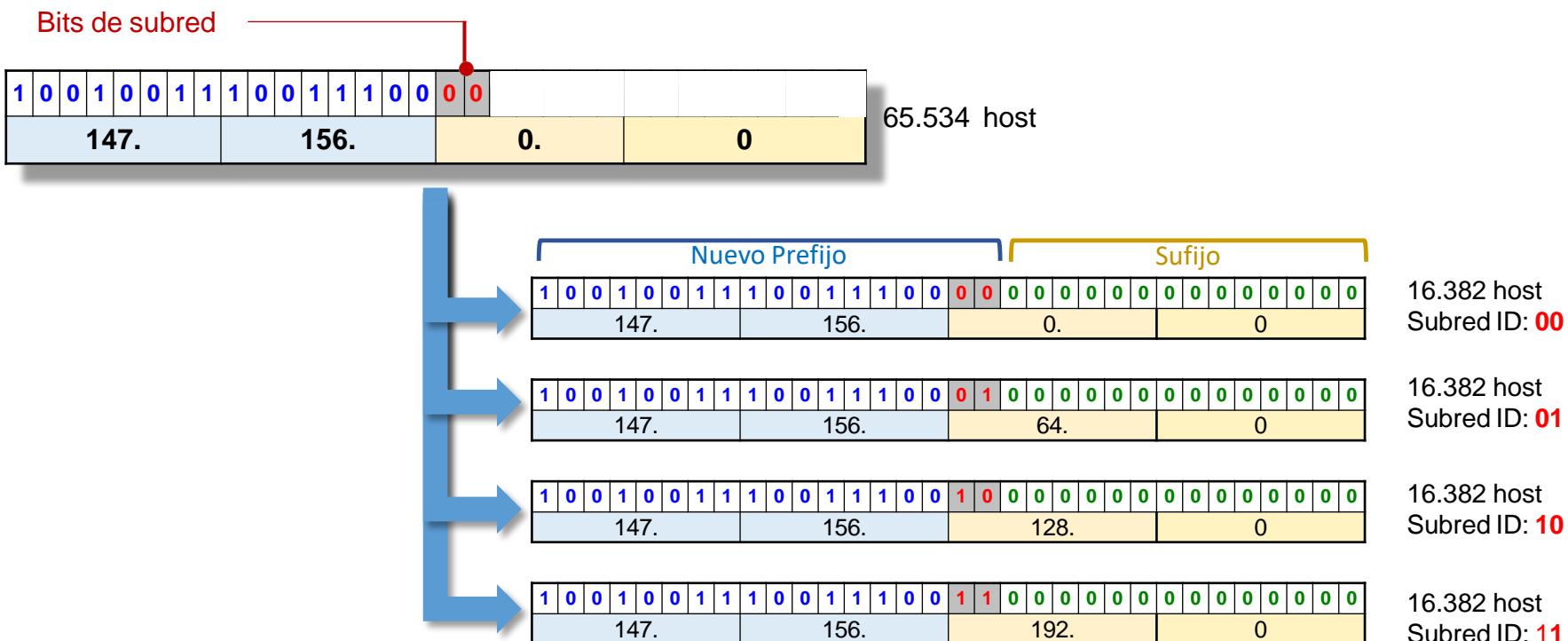
Subredes

Caso de estudio



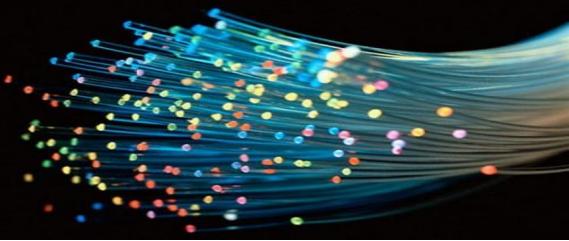
■ Subneteo de una clase B en 4 subredes de 16.382 direcciones

- Red original 147.156.0.0. Máscara por defecto 255.255.0.0
- 2 Bits de subneteo: los de peso 15 y 14
- Nueva Máscara: /18 (255.255.192.0)
- **147.156.subred.0**: identifica a cada subred. En este caso **subred=0, 64, 128 y 192**



El subneteo de tamaño variable

VLSM (*Variable Length Subnet Mask*)



El subneteo de tamaño variable es otra de las soluciones adoptadas para evitar el agotamiento de direcciones IP, como el CIDR, el NAT y las direcciones IP privadas



Se ha estudiado anteriormente que el método CIDR divide las redes de forma homogénea (mismo tamaño) en todo el espacio de direcciones, lo cual provoca, inevitablemente, el desperdicio de direcciones.

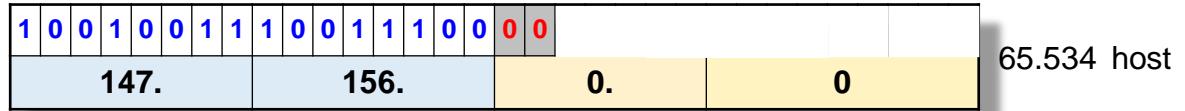
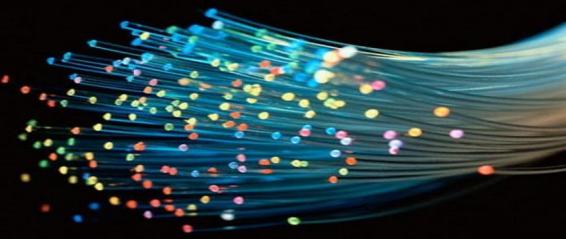
La técnica VLSM puede dividir una red en subredes de diferentes tamaños, utilizando máscaras de subred de tamaño variable (VLSM).

El concepto básico de VLSM es muy simple:

Se toma una red y se divide en subredes fijas, luego se toma una de estas subredes y se vuelve a dividir, tomando bits "prestados" de la porción de hosts, ajustándose a la cantidad de hosts requeridos por cada segmento de la red.

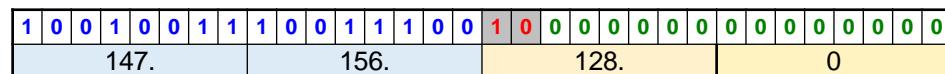
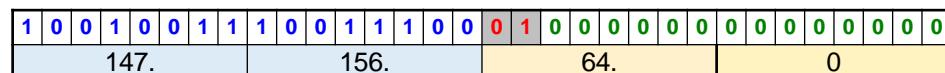
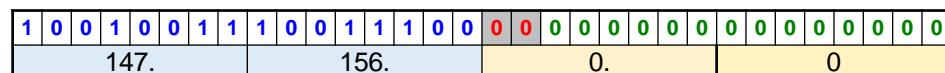
El subneteo de tamaño variable

Caso de estudio



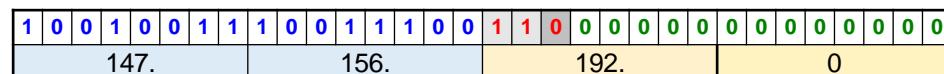
Primera división:

Red de clase B se fragmenta en 4 subredes



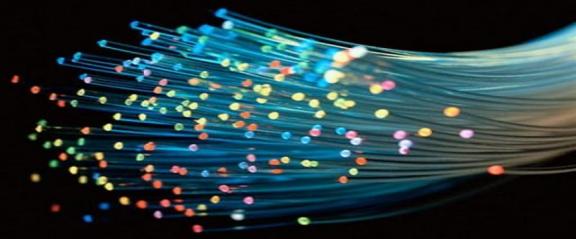
Segunda división:

La subred 147.156.0.192/18 se fragmenta en 2 subredes /19



Agregación de rutas

Superneteo (*Supernetting*)



La formación de superredes es una técnica preventiva para evitar la ineficiencia de la asignación de rangos IP y evitar la sobrecarga de las tablas de encaminamiento de los routers



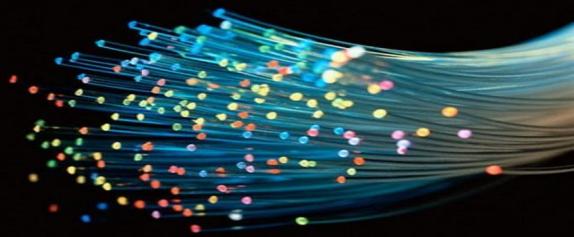
Una **superred**, es una red IP que está formada por la combinación (agrupación) de dos o más redes o subredes contiguas con un prefijo CIDR común, de tal forma que el prefijo de enrutado de la superred comprende los prefijos de las redes que la constituye.

El procedimiento de superneteo o agregación de rutas consiste en:

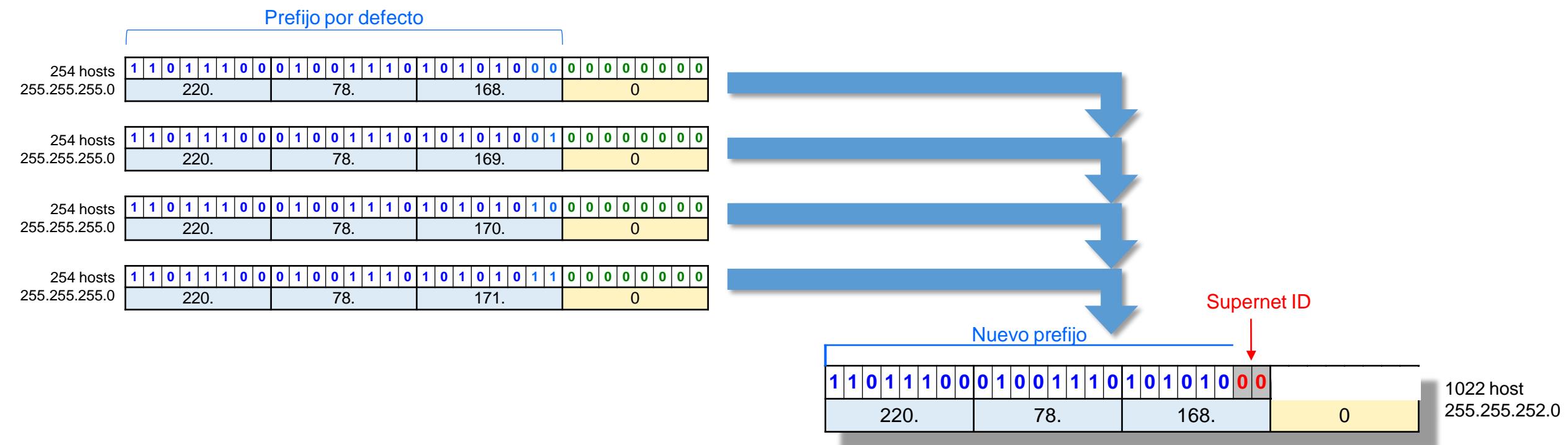
Se toman dos o más bloques de direcciones de red numéricamente contiguas (consecutivas) y se consolidan en una sola dirección de red más grande., con una máscara mas corta.

Super-redes

Caso de estudio



- Agrupación de 4 redes de clase C en una superred de 1024 direcciones
 - Máscara por defecto de las redes de clase C: 255.255.255.0
 - 2 Bits de superred: los de peso 9 y 10
 - Nueva Máscara: /22 (255.255.252.0)



Direcciones IP privadas



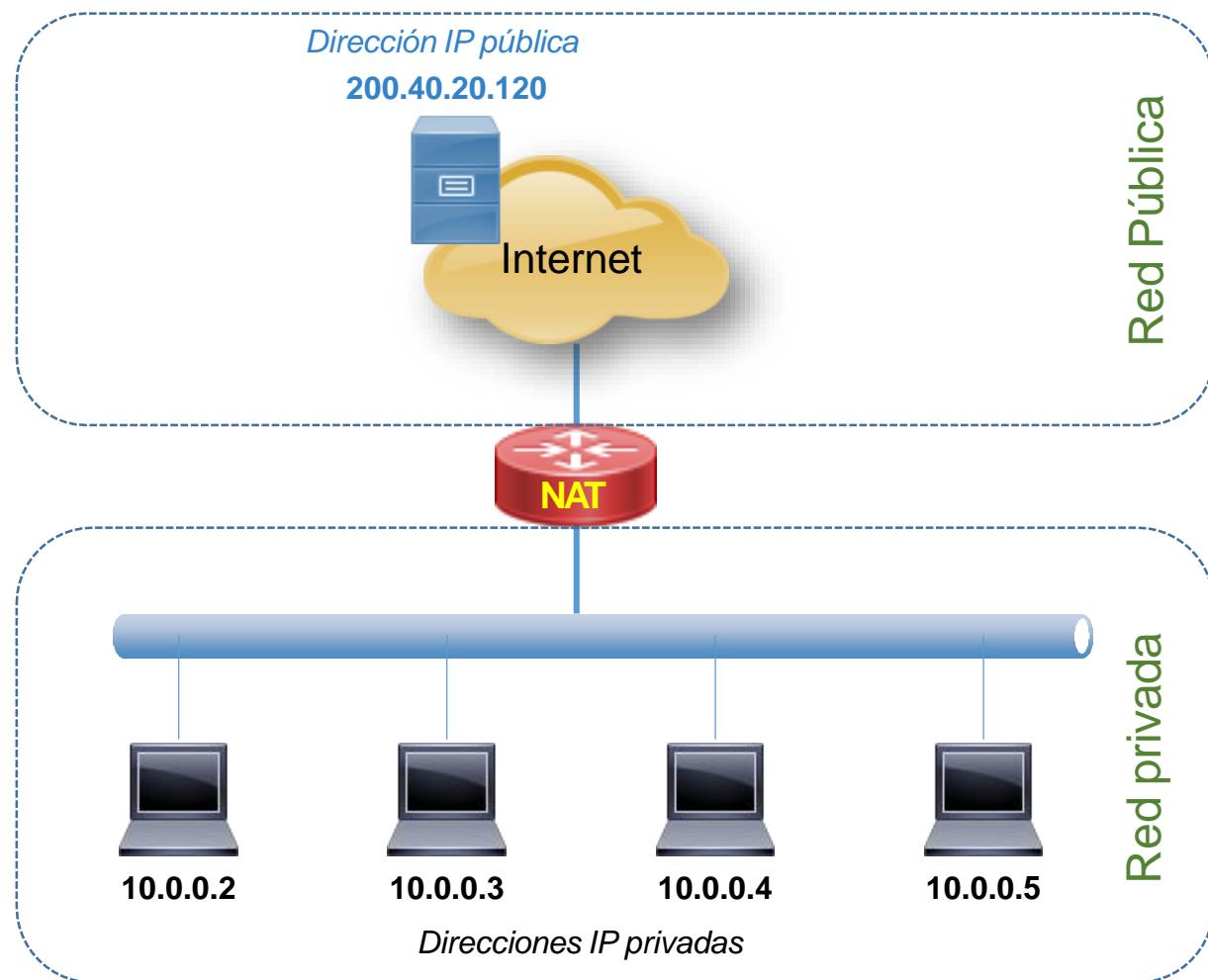
■ Existen cuatro rangos de direcciones IP que han sido declarados como privados

- Esto significa que las direcciones incluidas en esos rangos son “no enrutables” o “alcanzables” desde Internet
- A diferencia de las **direcciones públicas**, las direcciones privadas no están controladas por ICANN
- Las **direcciones privadas** pueden aplicarse a dispositivos que no requieren conexión a Internet (impresoras, switches, etc.) y redes de usuarios o servidores que no queremos que accedan a Internet o redes que acceden a Internet a través de otros mecanismos (NAT-PAT, Proxy, etc.)

	Desde				Hasta				<u>Mascara por defecto</u>				<u>Número de redes</u>
A	10 .	0 .	0 .	0	10 .	255 .	255 .	255	255.	0.	0.	0.	1 Red(es)
B	169 .	254 .	0 .	0	169.	254.	255.	255	255.	255.	0.	0.	1 Red(es)
B	172 .	16 .	0 .	0	172.	31.	0.	0	255.	255.	0.	0.	16 Red(es)
C	192.	168.	0.	0	192.	168.	255.	0	255.	255.	255.	0.	256 Red(es)

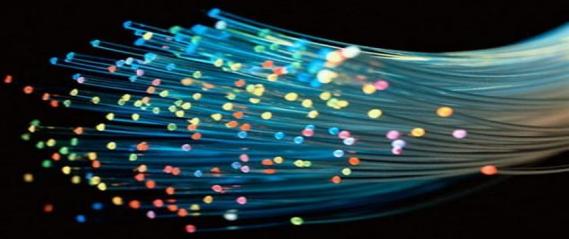
NAT (*Network Address Translation*)

- NAT es el mecanismo utilizado por los encaminadores IP para intercambiar paquetes entre dos redes que asignan mutuamente direcciones incompatibles
 - Consiste en convertir, en tiempo real, las direcciones utilizadas en los paquetes transportados
 - Su uso más común es permitir utilizar direcciones privadas (RFC 1918) para acceder a Internet

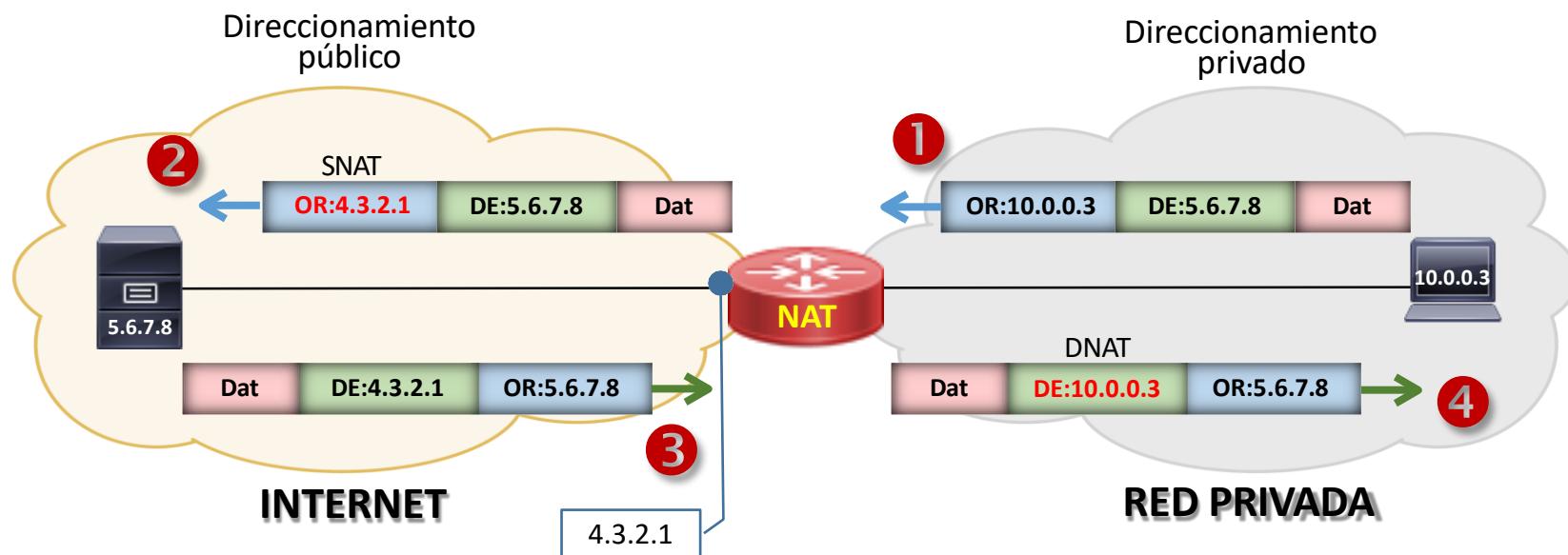


NAT (*Network Address Translation*)

Funcionamiento



- Consiste en sustituir, en tiempo real, la dirección IP de origen en los paquetes que van desde una estación privada a Internet, y sustituir la dirección de destino IP en los paquetes que pasan de Internet a dicha estación
 - 1) Desde la red privada se emite un paquete de petición con destino a un servidor situado en Internet
 - 2) Antes de que pase a Internet, el router, cambia la dirección de origen por su IP pública
 - 3) El servidor elabora el paquete de respuesta con direcciones públicas
 - 4) El router traducirá la dirección IP de destino del paquete (IP del router) por la dirección privada del host.





4.2. Direccionamiento IPv6

IPv6. Motivaciones

IPv6. Direccionamiento

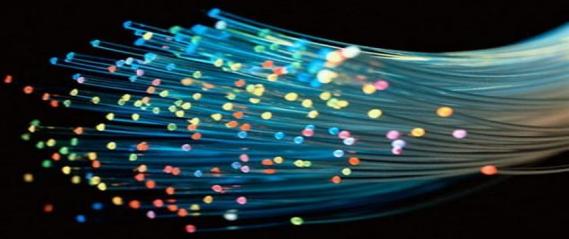
IPv6. Asignación

IPv6. Notación

IPv6. Tipos de Direccionamiento

IPv6

Motivaciones



■ Razones que justifican IPv6

- Agotamiento de las direcciones
IPv4 (solo 4.294.967.296
direcciones)
- Las nuevas aplicaciones exigen
funcionalidades que IPv4 no
puede ofrecer (pe. Calidad de
servicio, seguridad, movilidad)
- Posibilidad de paquetes
superiores a 64 kb (jumbogramas,
hasta 4 GB)



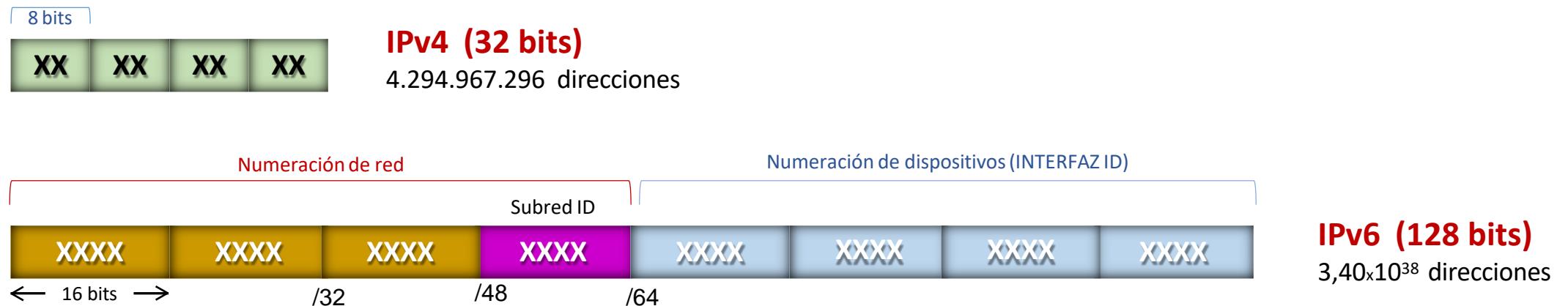
IPv6

Direccionamiento



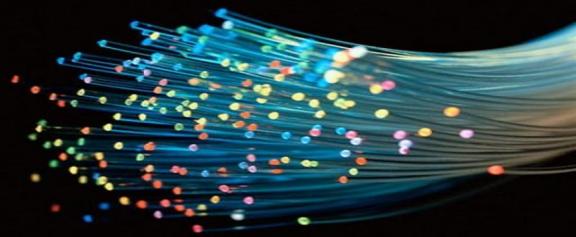
- El esquema de direccionamiento IPv6 se define en la RFC 4291

- 128 bits de longitud
- permite asignación jerárquica
- Numeración hexadecimal
- Usa los principios de enrutamiento sin clases (CIDR)



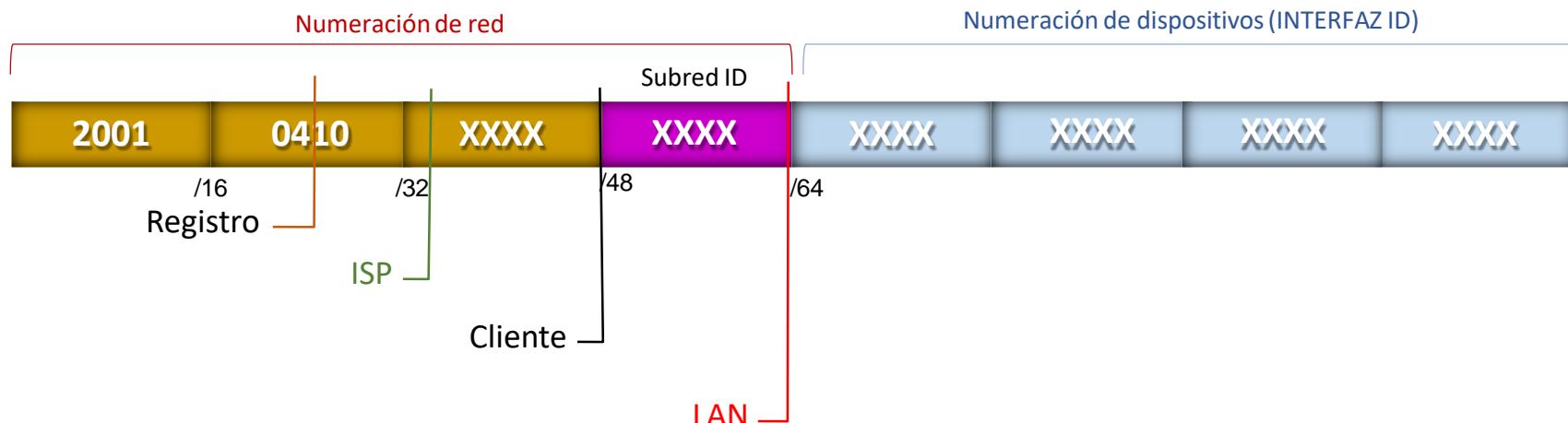
IPv6

Direccionamiento. Asignación

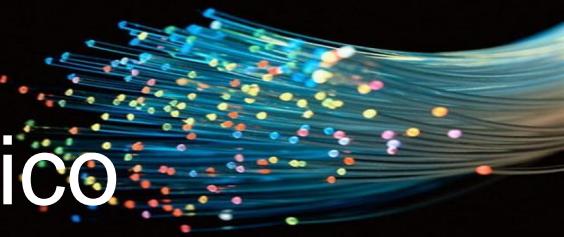


■ Política de asignación:

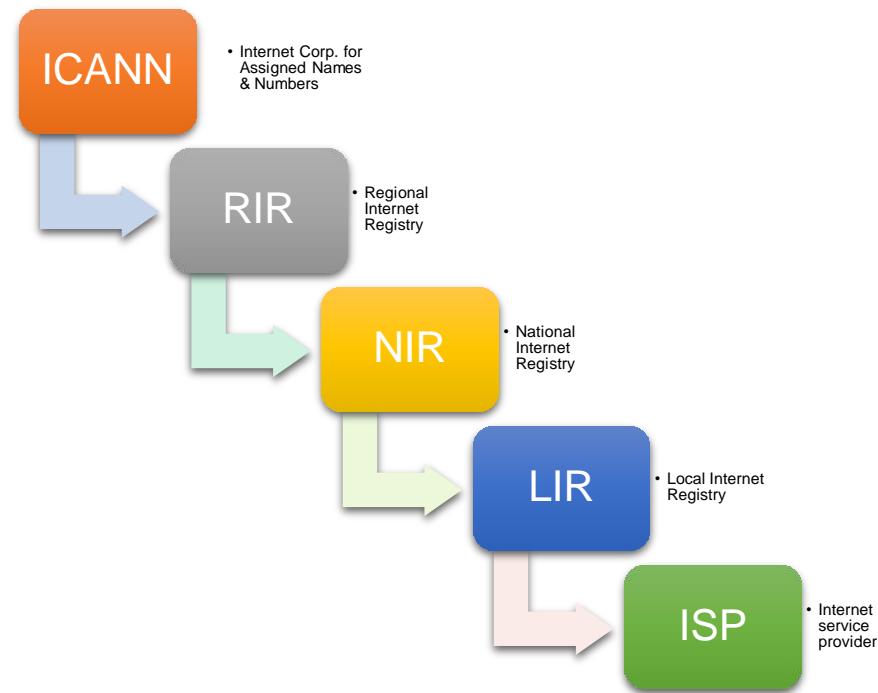
- IANA asigna 2001 :: /16 a los registros
- Cada registro se pone un prefijo /23 del IANA
- Todos los ISP tienen un prefijo /35
- Con esta política, un registro puede asignar un prefijo /32 a un proveedor de Internet IPv6
- A continuación, el ISP puede asignar un prefijo /48 a cada cliente



La gestión del direccionamiento público

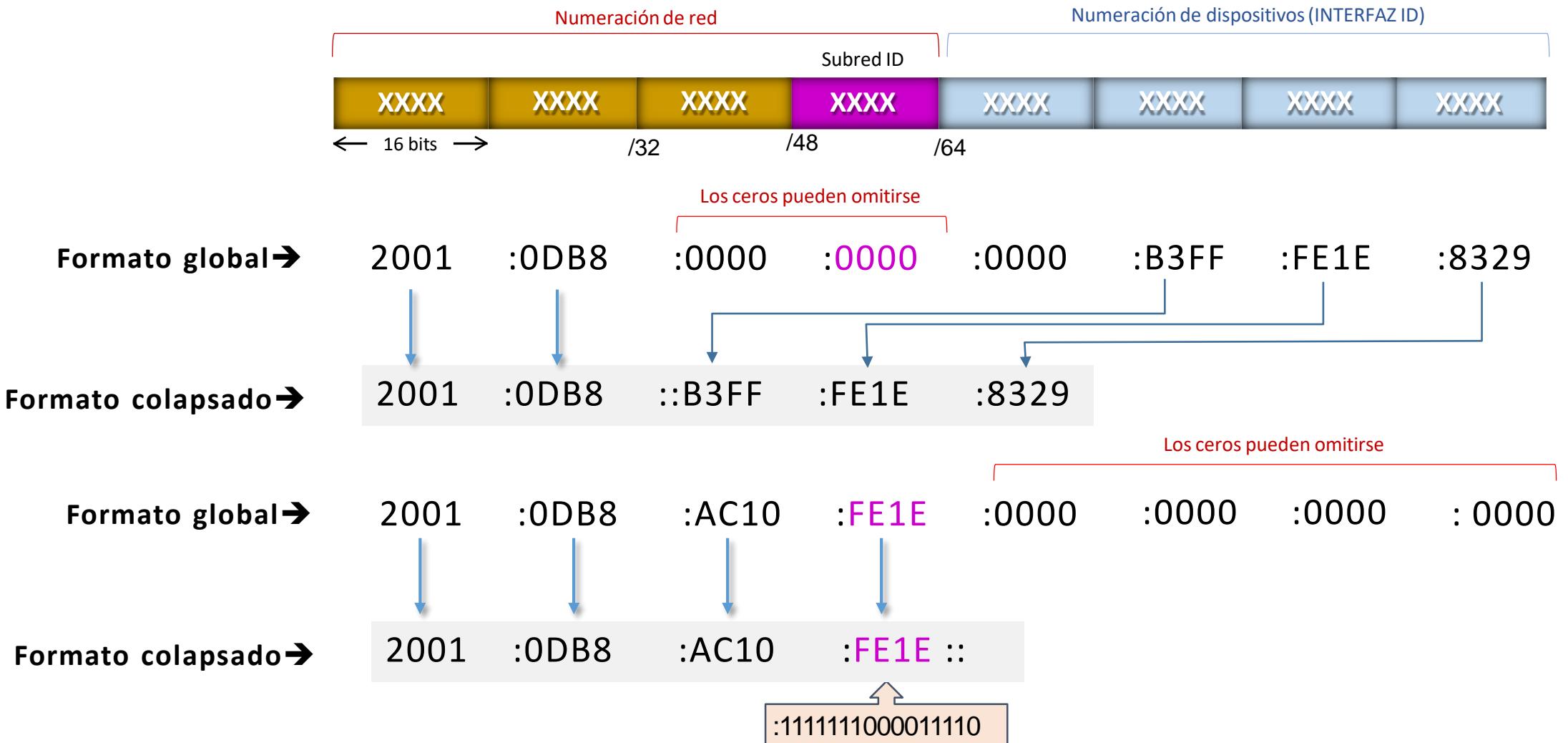
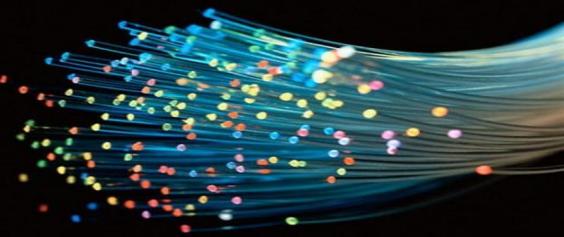


La gestión del espacio público de direcciones de Internet se coordina mundialmente a través de varias organizaciones, siguiendo una estructura jerárquica: **ICANN** es la que vela a nivel mundial por la gestión de dichos recursos. En Europa es **RIPE** la RIR encargada de gestionar estas direcciones y, por debajo de ella, están los Registros de Internet Nacionales (**NIRs**), y locales (**LIRs**), como **RedIRIS** en España.



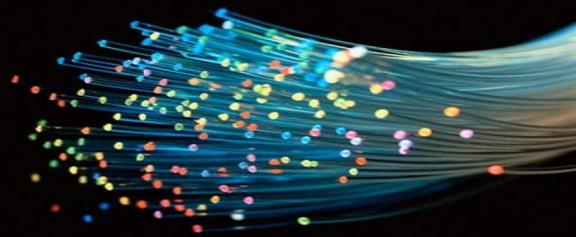
IPv6

Direccionamiento. Notación



IPv6

Direccionamiento. Tipos



■ Unicast:

- Identifican a una sola interfaz. El paquete se envía a una interfaz.

■ Anycast:

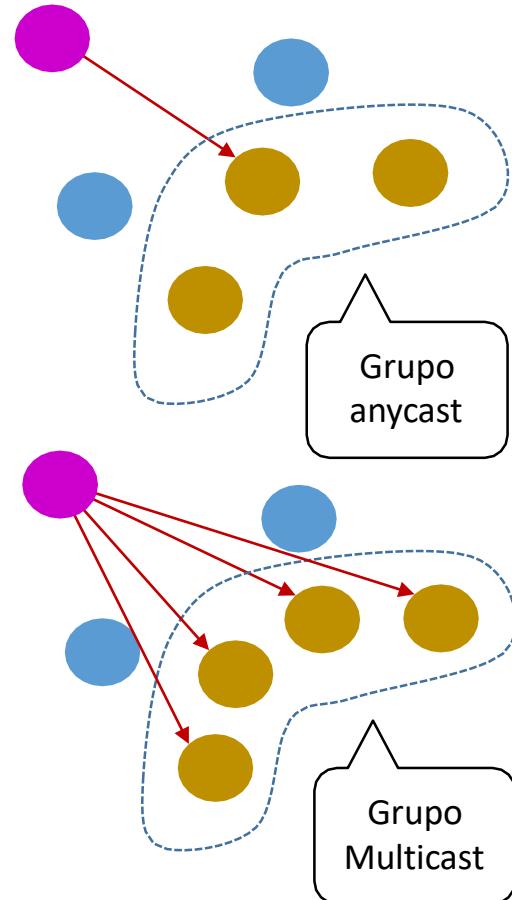
- Identifica a un conjunto de interfaces. Una dirección anycast es asignada a un grupo de interfaces, normalmente de nodos diferentes. Un paquete enviado a una dirección anycast se entrega únicamente a uno de los miembros, típicamente el host con menos coste (pe. el mas cercano), según la definición de métrica del protocolo de encaminamiento.

■ Multicast:

- Identifica un grupo de interfaces. Cuando un paquete es enviado a una dirección multicast es entregado a todos las interfaces del grupo identificados con esa dirección.

■ Broadcast:

- No se implementa



4.3. El datagrama IP

El nivel IP

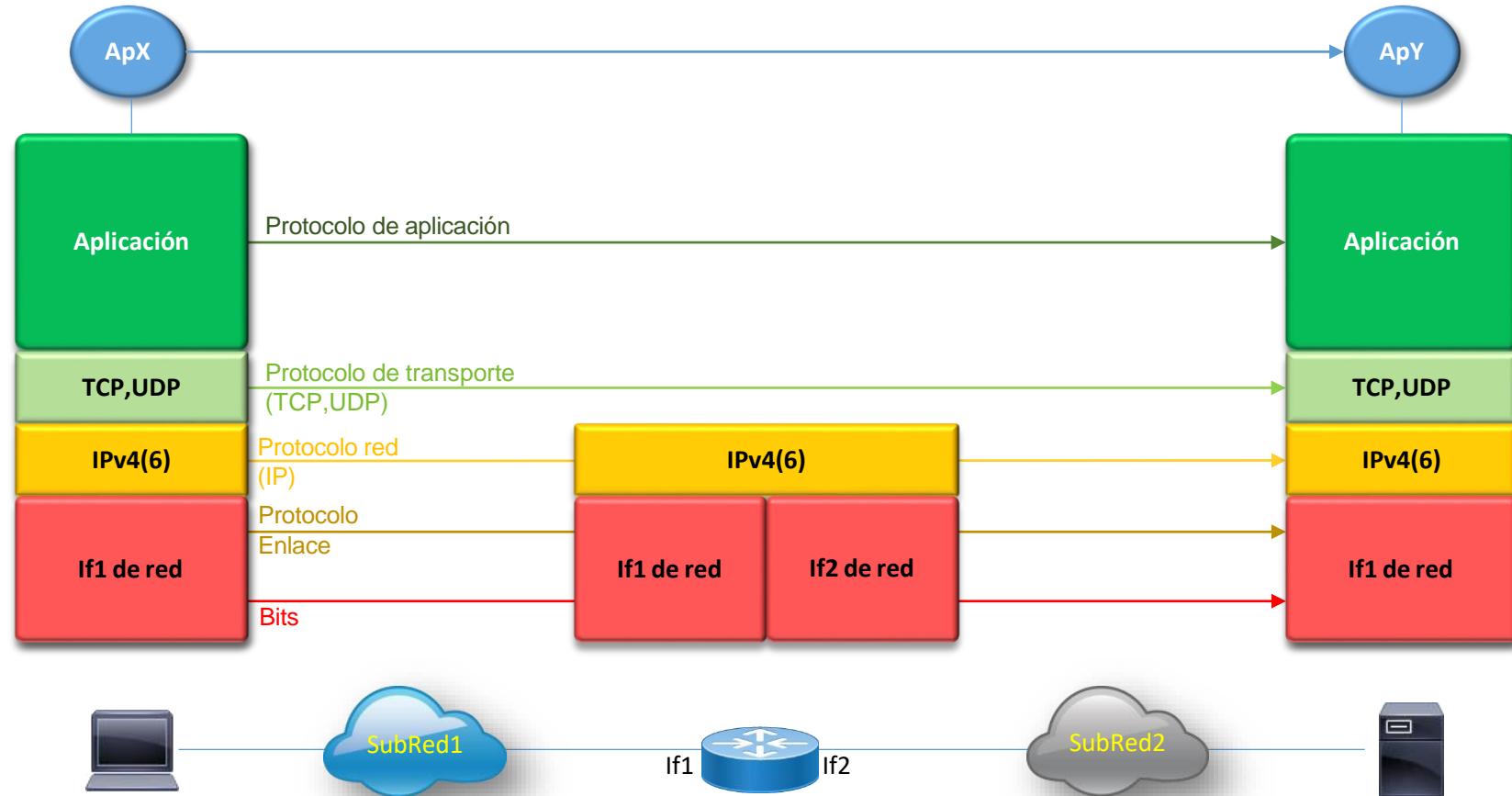
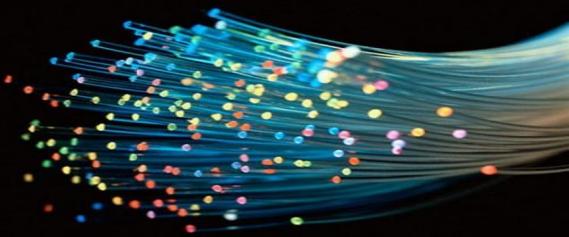
Las funciones de la capa IP

El datagrama IPv4

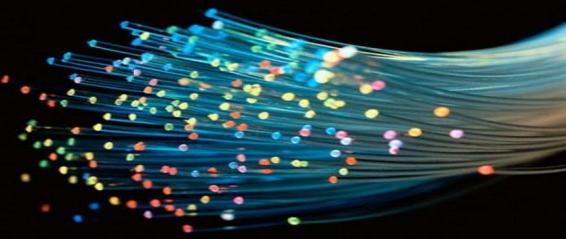


El nivel IP

Arquitectura TCP/IP



Las funciones de la capa IP



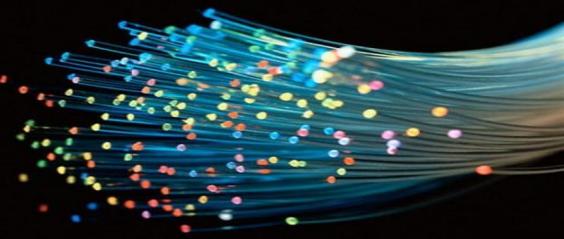
La capa IP ofrece una **comunicación extremo a extremo no orientada a conexión**, independientemente de las redes por las que se pase y **sin ninguna garantía** sobre la llegada correcta paquetes

(no hay corrección de errores ni control de congestión ⇒ han de ser corregidos por el nivel superior)

■ Funciones

- Direccionamiento lógico (dirección IP)
- Cómo almacenar y reenviar datagramas
- Segmentación y reensamblado

El datagrama IPv4 [1]

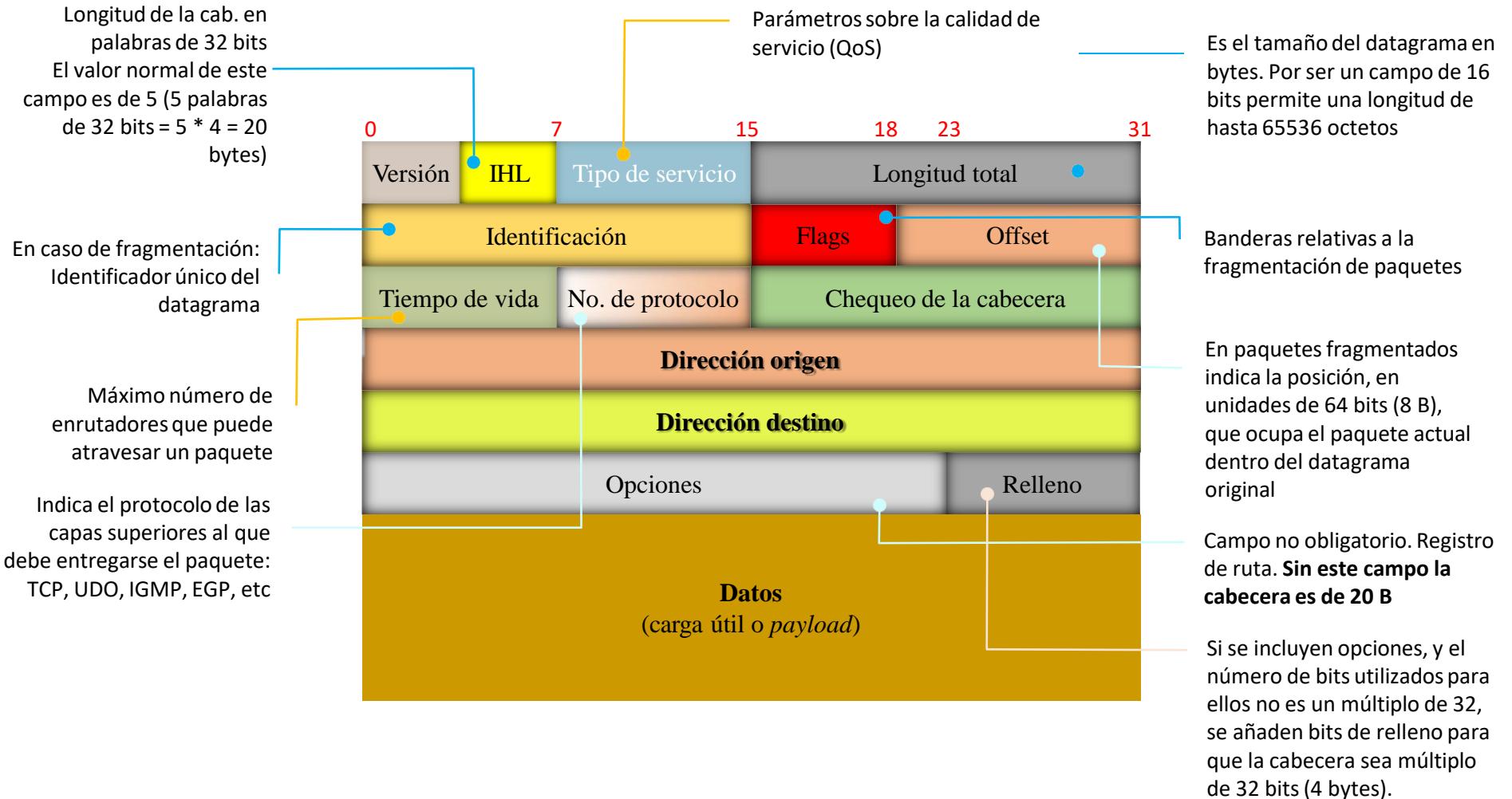
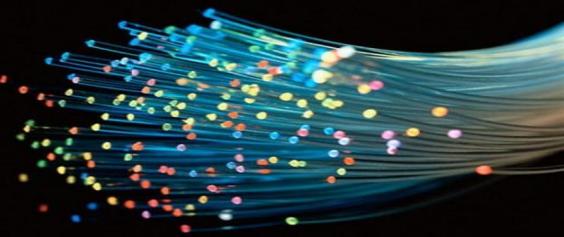


- Para poder encaminar los datagramas, el nivel IP añade sus propias cabeceras
 - Por tanto, el datagrama IP tiene dos partes: cabecera y carga útil (datos: protocolo superior encapsulado)
 - Su tamaño puede variar desde 20 hasta 64K octetos



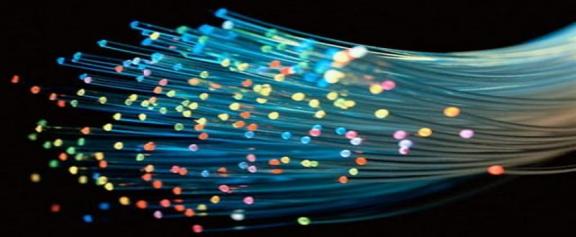
El datagrama IPv4 [2]

Formato de la cabecera

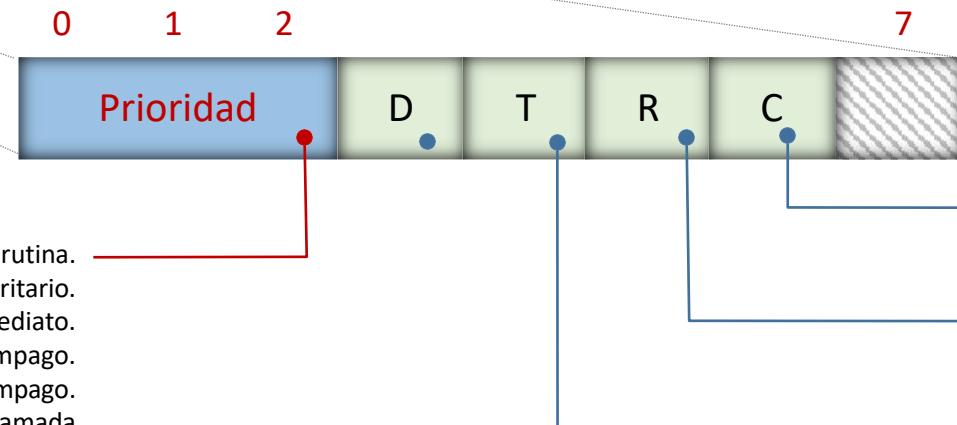
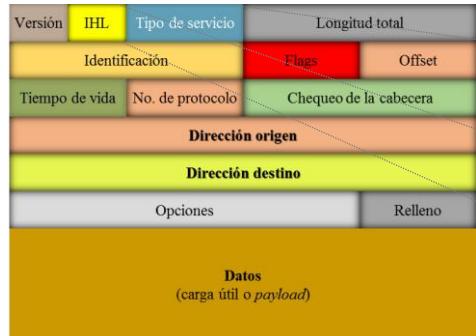


El datagrama IPv4 [3]

El campo *tipo de servicio*



- El Tipo de Servicio, determina una serie de parámetros sobre la calidad de servicio (QoS) deseada durante el tránsito por la red
 - Lo establece la entidad que envía el datagrama



000: De rutina.
001: Prioritario.
010: Inmediato.
011: Relámpago.
100: Invalidación relámpago.
101: Procesando llamada crítica y de emergencia.
110: Control de trabajo.
111: Control de red.

Delay:
Normal (0)
Mínimo (1)

Coste:

Normal (0)
Mínimo (1)

Fiabilidad (Reliability):

Normal (0)
Máxima (1)

Throughput:

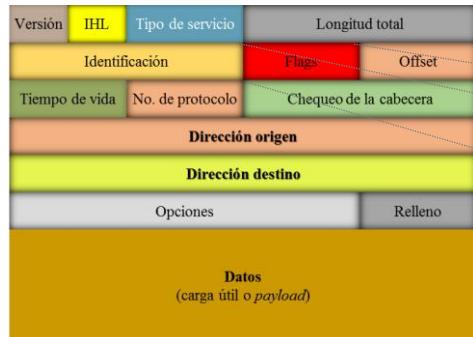
Normal (0)
Máxima (1)

El datagrama IPv4 [4]

El campo *flags*



- Cuando un datagrama IP es demasiado grande para la unidad de transmisión máxima (MTU) de la tecnología de capa de enlace de datos subyacente, debe ser fragmentado antes de que pueda ser enviado a través de la red
 - El campo *flags*, de tres bits, se utiliza para permitir el montaje correcto del mensaje fragmentado
 - El proceso de fragmentación es *invisible* para las capas superiores



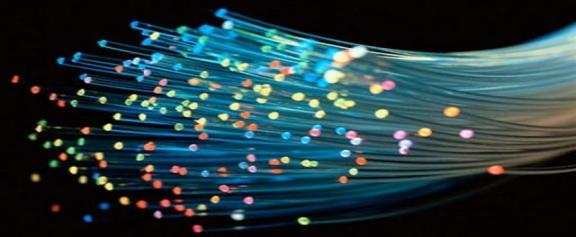
Reservado:
Debe ser cero

More fragments:
Indicación de que es el último fragmento (0)
Indicación de que hay mas fragmentos (1)

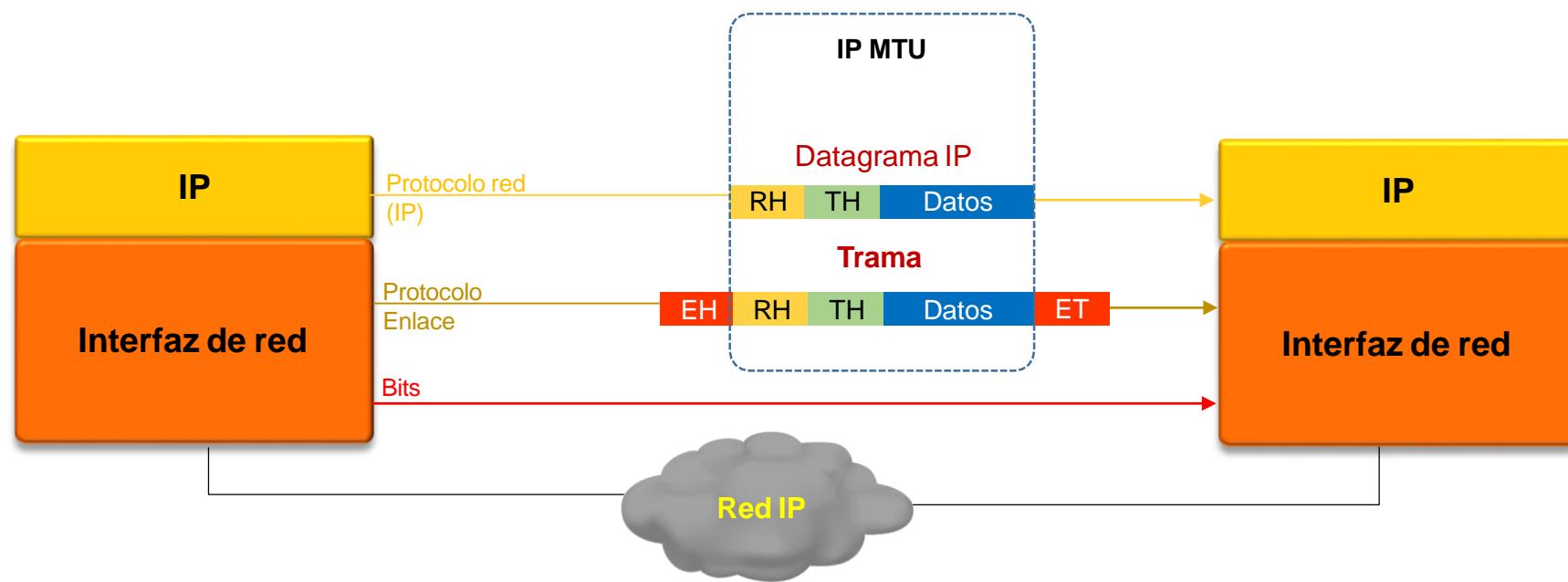
Don't fragment:
Se puede fragmentar (0)
No se puede fragmentar (1)

El datagrama IPv4 [5]

MTU

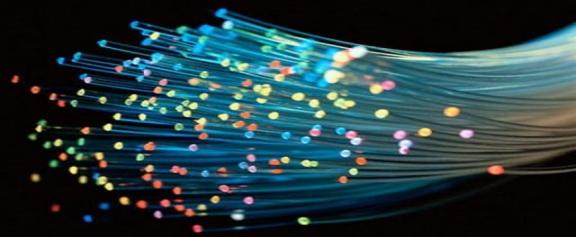


- El protocolo IP fue diseñado para su uso con una amplia variedad de tecnologías de transmisión (*Ethernet, ATM, FR, LL, etc.*) y aunque la longitud máxima teórica de un datagrama IP es de 64KB, la mayoría las tecnologías de los enlaces imponen un límite máximo de los datagramas, ese límite se llama abreviadamente **MTU**
 - Dicho de otro modo, la **Unidad Máxima de Transferencia** (*Máximum Transfer Unit - MTU*) expresa en bytes la unidad de datos (*payload o carga útil*) más grande que puede enviarse en el un protocolo de enlace subyacente

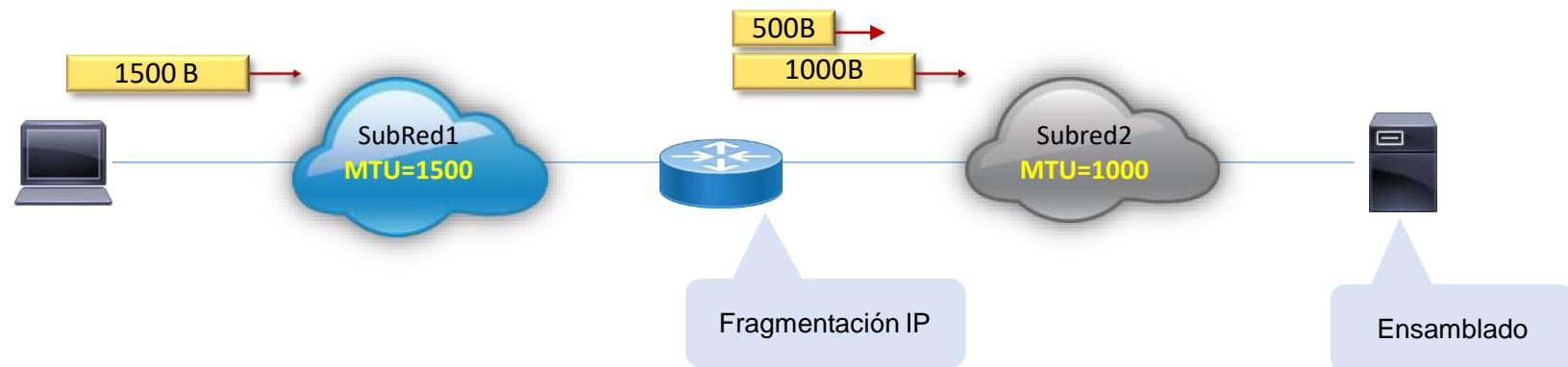


El datagrama IPv4 [6]

MTU y fragmentación

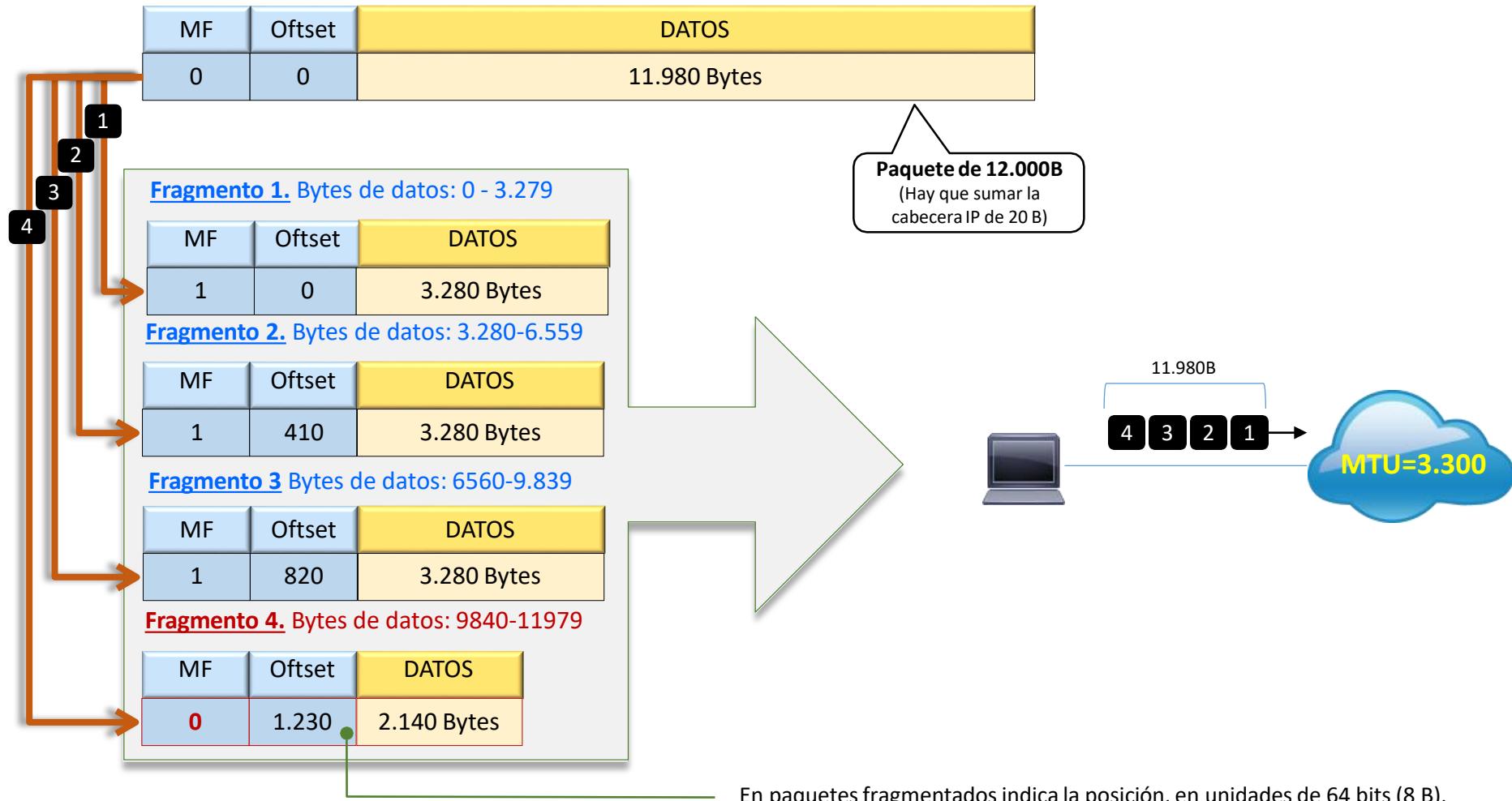
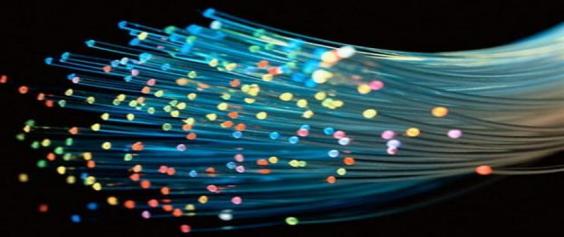


- El diseño de IP, permite a este acomodarse a los diferentes MTUs al habilitar que los routers puedan fragmentar datagramas IP si es necesario
 - La estación receptora es responsable de volver a ensamblar los fragmentos para rehacer el datagrama IP original.



El datagrama IPv4 [7]

Ejemplo de fragmentación

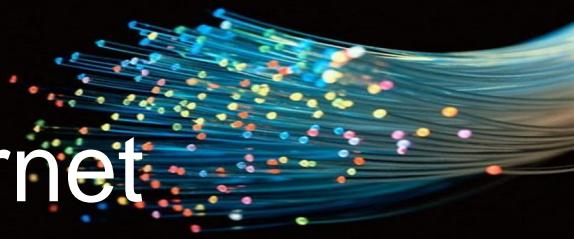


4.4. El Protocolo ICMP

Protocolo de mensajes de control de Internet
Tipos de mensajes
Formato
Mensajes de error
Mensajes de diagnóstico



Protocolo de mensajes de control de Internet



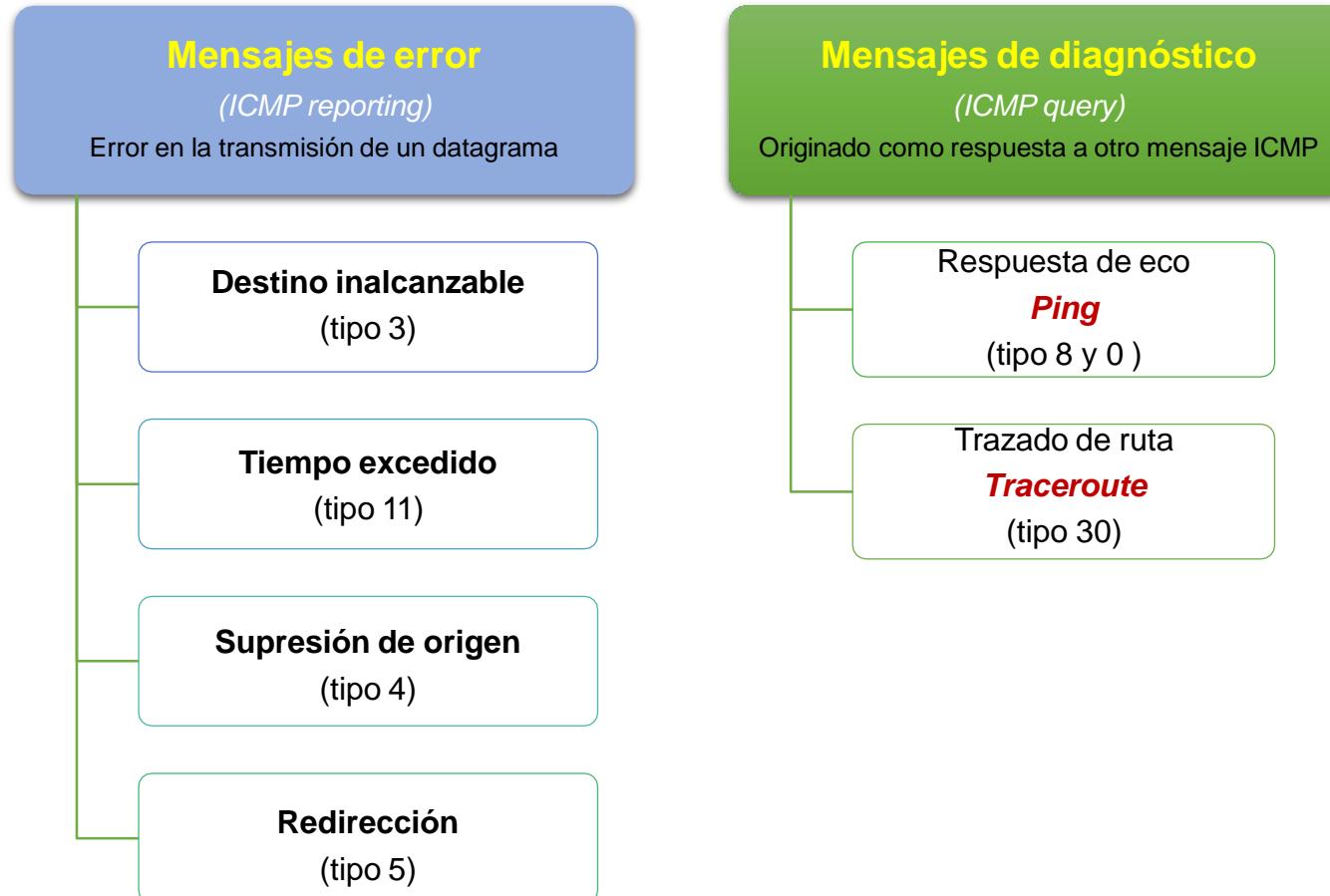
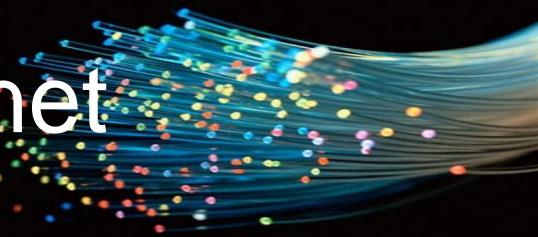
El protocolo IP, que se usa para la transferencia de datos, está acompañado por otros protocolos que se usan a nivel de red, como son **ARP, DHCP e ICMP**.

■ **ICMP (Internet Control Messages Protocol)** se utiliza, fundamentalmente, para la gestión de mensajes de error y otras condiciones que requieran atención.

- Los mensajes ICMP se activan, generalmente, por el nivel IP o por protocolos de nivel superior (UDP, TCP).
- Son generados por el host o router que detecta el problema o situación extraordinaria y dirigidos al host o router que aparece en el campo dirección origen del datagrama que causó el problema.
- Los mensajes ICMP viajan por la red como datagramas IP (con el valor 1 en el campo Protocolo), sujetos en los routers a las mismas reglas que cualquier otro datagrama.
- **ICMP usa IP como si fuera un protocolo de nivel superior**, sin embargo se implementa con el módulo IP

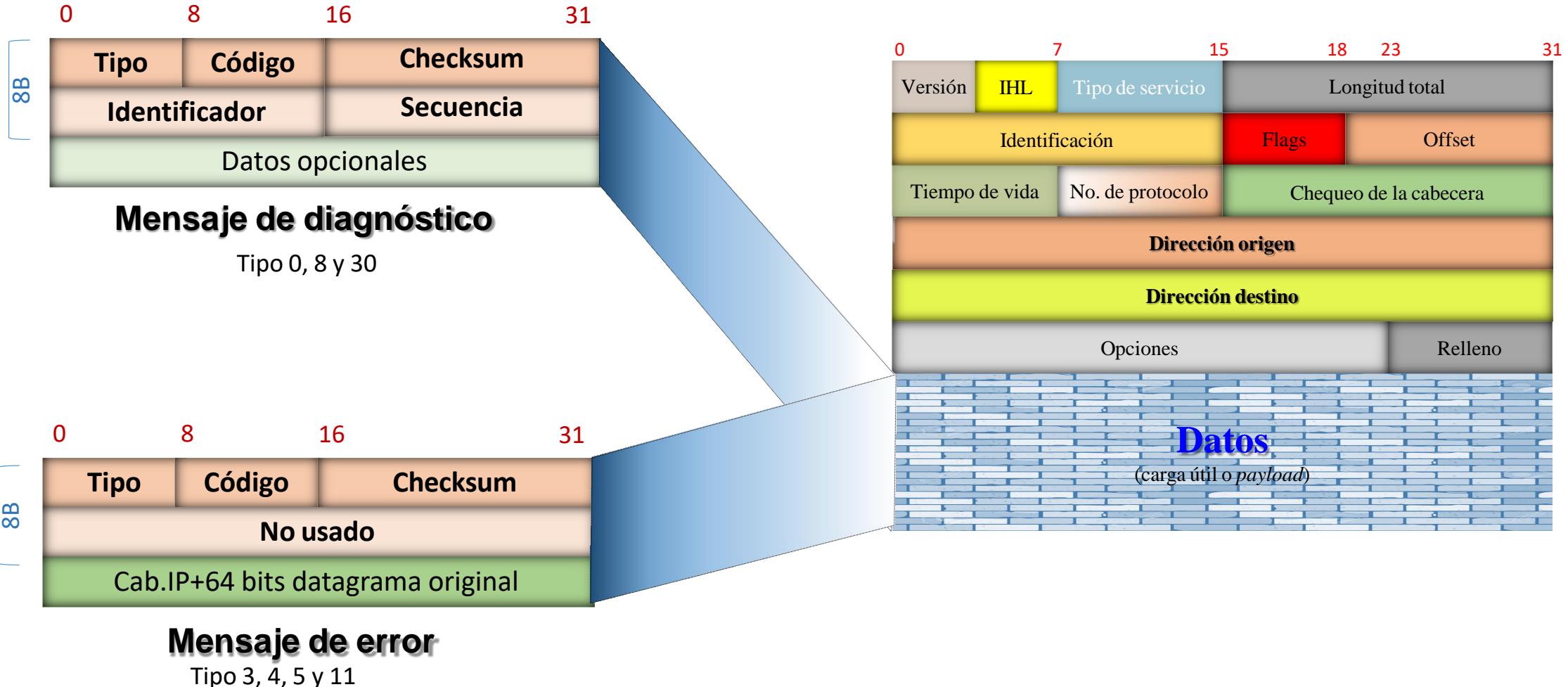
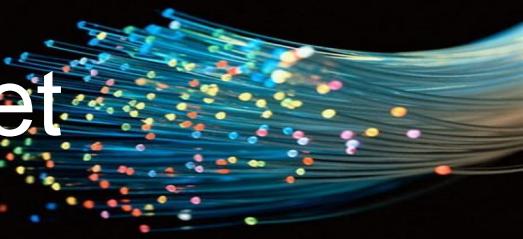
Protocolo de mensajes de control de Internet

Tipos de mensajes



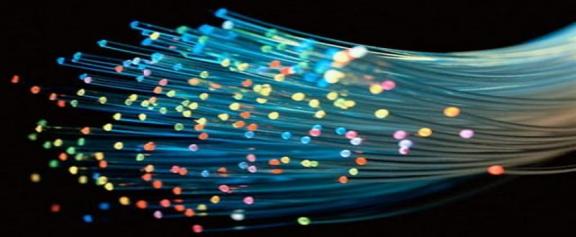
Protocolo de mensajes de control de Internet

Formato



Mensajes ICMP

Mensajes de error [1]



■ **Destination unreachable** (Destino inalcanzable:Tipo 3)

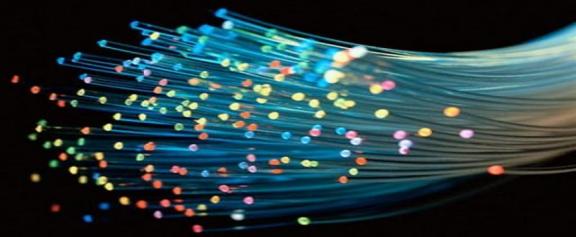
- El campo Datos contiene la cabecera IP y los primeros 8 bytes de la carga útil del datagrama original. Un router puede emitir este mensaje si no se puede entregar el datagrama en su destino porque:
 - ✓ El router se encuentra con un datagrama con el bit DF =1 y que no cabe en la MTU de la red por la que ha de enviarlo.
 - ✓ El router no encuentra en sus tablas ninguna ruta por la que pueda llegar a la dirección de destino de un datagrama.

■ **Source Quench** (Supresión de origen: Tipo 4). Aviso de descarte por congestión.

- Permite a los routers solicitar una reducción en el tráfico generado por los hosts en caso de congestión

Mensajes ICMP

Mensajes de error [2]



■ **Time exceeded for datagram** (tipo 11)

- Aviso de un descarte por exceso de tiempo en el sistema (TTL=0). No se usan los cuatro bytes finales de la cabecera; el campo Datos contiene la cabecera IP y los primeros 8 bytes de la carga útil del datagrama original.

■ **Redirect** (Tipo 5)

- Se utiliza para alertar al host emisor cuando se sospecha que un paquete se está encaminando incorrectamente.
 - ✓ Los cuatro bytes finales de la cabecera contienen la dirección del router al que redireccionar el tráfico; el campo Datos contiene la cabecera IP y los primeros 8 bytes de la carga útil del datagrama original

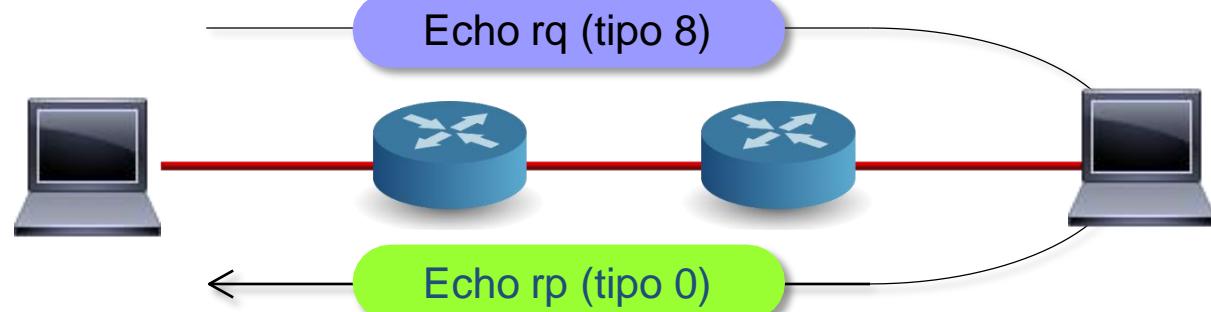
Mensajes ICMP

Mensajes de diagnóstico. *Ping*



■ *Ping* (tipo 8 y 0)

- Es una solicitud de eco
- El destino devuelve el mismo mensaje que se le envió; después el emisor comprueba el campo de datos recibido con el transmitido
- Comprueba que la comunicación entre emisor y receptor es posible



```
C:\>ping 172.26.0.3

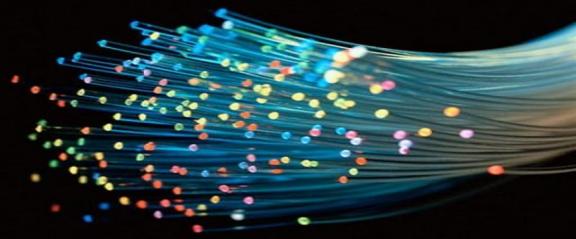
Haciendo ping a 172.26.0.3 con 32 bytes de datos:
Tiempo de espera agotado para esta solicitud.

Estadísticas de ping para 172.26.0.3:
Paquetes: enviados = 4, recibidos = 0, perdidos = 4
(100% perdidos)
C:\>
```

A yellow callout bubble points from the word "perdidos" in the statistics to a separate text box containing the message "No hay respuesta".

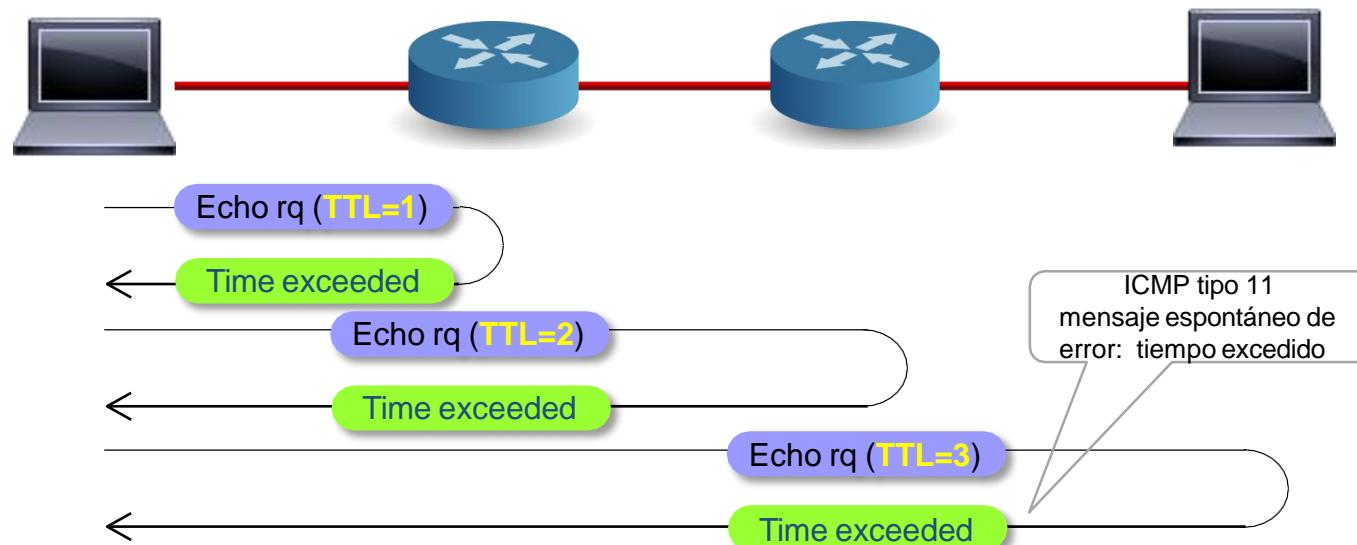
Mensajes ICMP

Mensajes de diagnóstico. *Traceroute*



■ Traceroute (tipo 30)

- Nos dice la ruta seguida por los datagramas en una conexión.
- Para lograr esto, se envían **echos** sucesivos con diferentes TTLs. Primero con TTL a 1. Esto ocasiona que el primer router envíe un ICMP de descarte por TTL=0, pero además incluirá su dirección IP. Luego se envía otro con TTL=1,2,... hasta que se reciba una respuesta de “traza completa”





4.5. Encaminamiento

El encaminamiento IP

Concepto de ruta

La tabla de encaminamiento

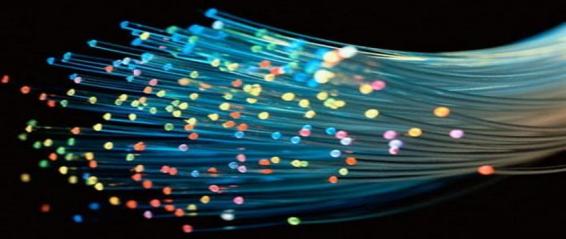
Transmisión directa de datagramas

Transmisión indirecta de datagramas

Tabla de rutas del host

Tabla de encaminamiento del router

Encaminamiento IP



Se denomina **encaminamiento** al proceso de reenviar un paquete basado en la dirección de destino.

■ Existen dos métodos de encaminamiento:

- Estático o no adaptativo

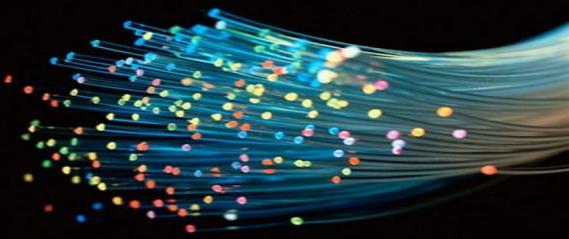
- ✓ No tienen en cuenta el estado de la red al tomar las decisiones de encaminamiento. Solo existe una ruta permanente por cada par origen-destino
- ✓ Las entradas de la tabla se crean manualmente, por medio de scripts que se ejecutan al inicializar el sistema, o por medio de comandos

- Dinámico o adaptativo

- ✓ Las decisiones de encaminamiento cambian en la medida que lo hacen las condiciones de la red
- ✓ Creadas y mantenidas de forma automática por los protocolos de *routing*

Encaminamiento IP

Estático vs. dinámico



Estático

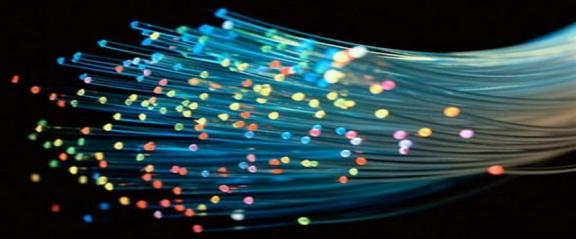
- Fijo
- Adecuado para casos simples
- Utiliza algoritmos de mínimo coste
- No influye el tráfico

Dinámico

- Variable en función de los valores aportados por los protocolos de enrutamiento
- Necesario en redes grandes
- Elementos de cambio: **fallos y congestión**

Encaminamiento IP

Concepto de ruta



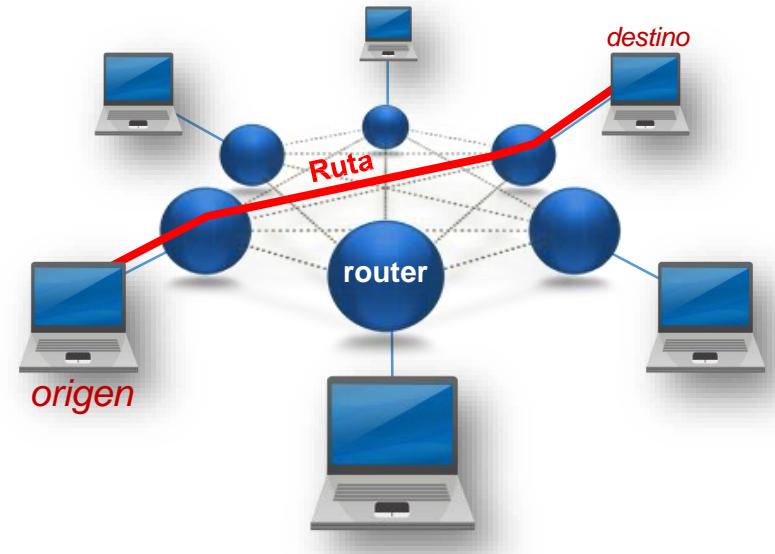
■ El **camino o ruta** se establece por medio de las diferentes tablas de encaminamientos de los distintos dispositivos (routers) que intervienen en la comunicación (a nivel IP).

■ Tipos de rutas

- **Directas** (Host a Host; ambos están en la misma subred). Los hosts se comunican directamente entre sí, sin necesidad de un dispositivo intermediario de capa de red.

- **Indirectas**

- ✓ A través de uno o más routers
- ✓ Se establecen salto a salto



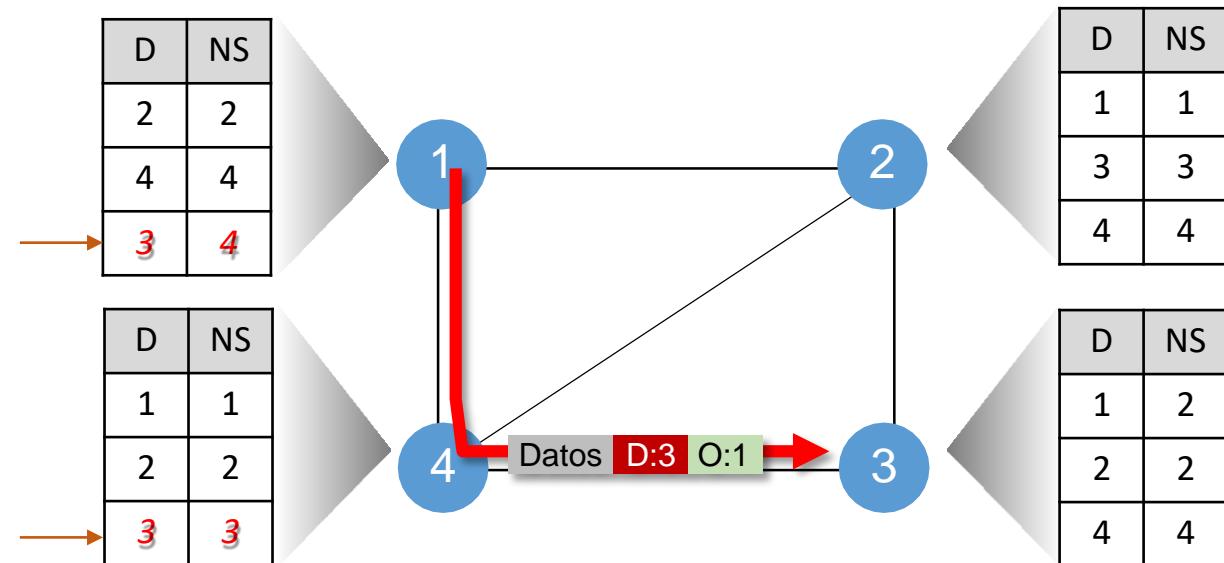
El encaminamiento IP

La tabla de encaminamiento



La tabla de **encaminamiento** se implementa mediante una **matriz** en la que se especifica, para cada destino, la **identidad del siguiente nodo en la ruta (Next hop)**.

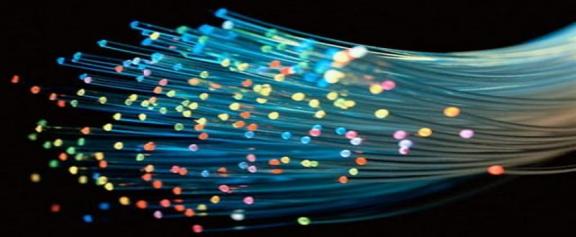
- Tanto los dispositivos finales (host) como los routers necesitan una tabla de encaminamiento para dirigir los paquetes a la red de destino correcta



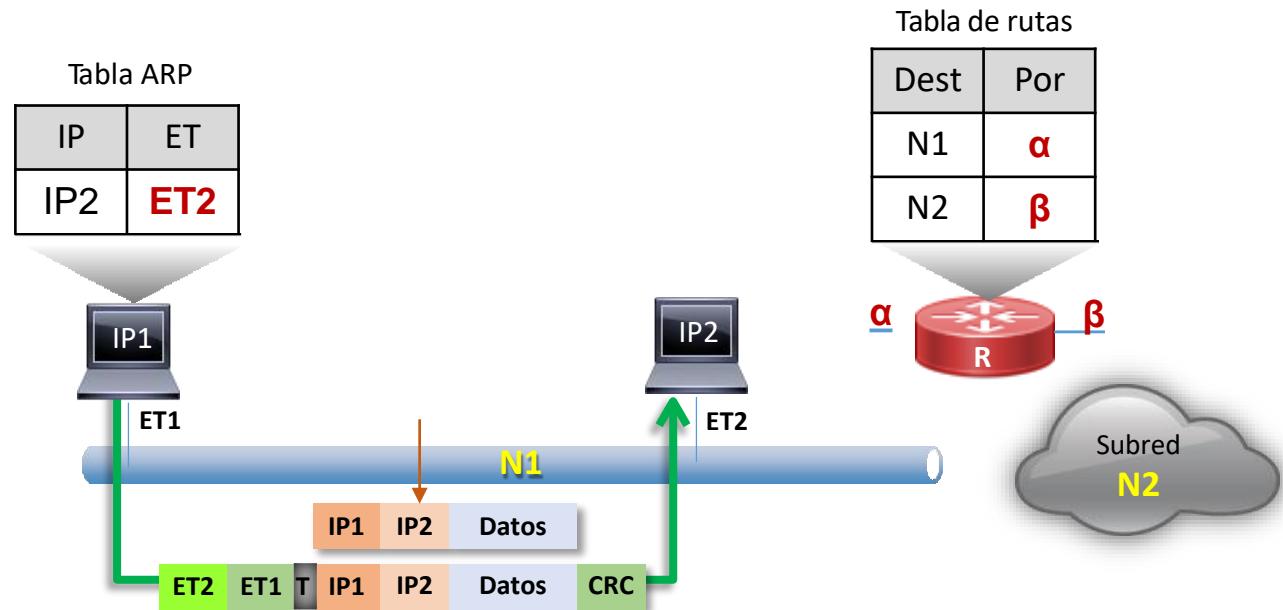
Nota: D es el destino y NS el nodo siguiente

El encaminamiento IP

Transmisión directa de datagramas. Encapsulamiento



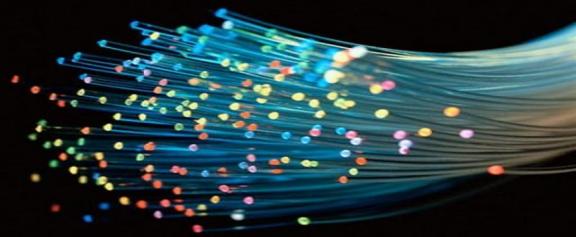
- Cuando los datagramas se envían entre dos host en la misma LAN (subred) se entregarán directamente desde el origen al destino
 - El primer host conoce tanto IP1 como IP2 y las incluye en la cabecera IP del datagrama que envía.
 - Para encapsular a nivel 2 se necesita conocer ET2 (dirección Ethernet): primero consultaría la tabla ARP, si no la encuentra entraría en juego el protocolo ARP



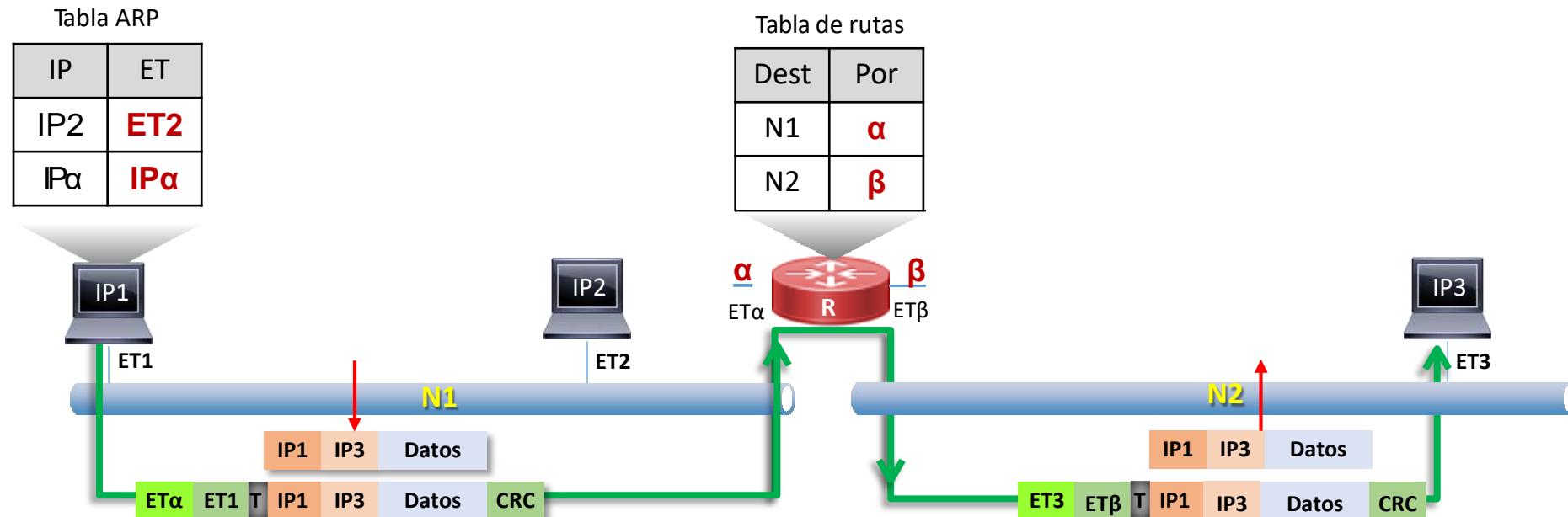
1. Esto se sabe gracias a la máscara

El encaminamiento IP

Transmisión indirecta de datagramas. Encapsulamiento

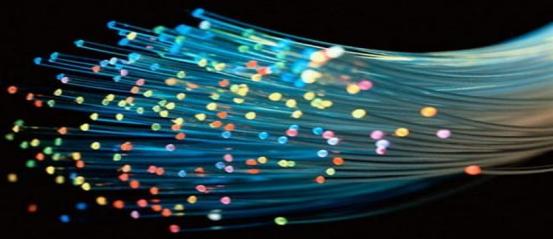


- El host origen sabe que IP3 no pertenece a su subred, por lo que envía el datagrama al router (con dirección IP3 de destino, pero encapsulado en una trama Ethernet con destino ET α)
 - En el router se consultan unas tablas de encaminamiento, que indican, partir de una dirección IP destino, a qué dirección IP hay que enviar



1. Esto se sabe gracias a la máscara

El encaminamiento IP



Transmisión directa de datagramas. Tabla de rutas del host

- Tanto los host como los routers tienen tabla de routing ya que han tomado decisiones de enrutamiento
 - Si el host de destino y de origen están en la misma subred¹, este envía el paquete **directamente al destinatario**
 - Si ambos prefijos (origen y destino) no coinciden entonces se envía el paquete a **su router por defecto**, el cual se encarga de enviar el paquete hacia su destino. El router por defecto siempre tiene un puerto conectado a la LAN que está el host.

Entrada:
Identificador de
la red de destino

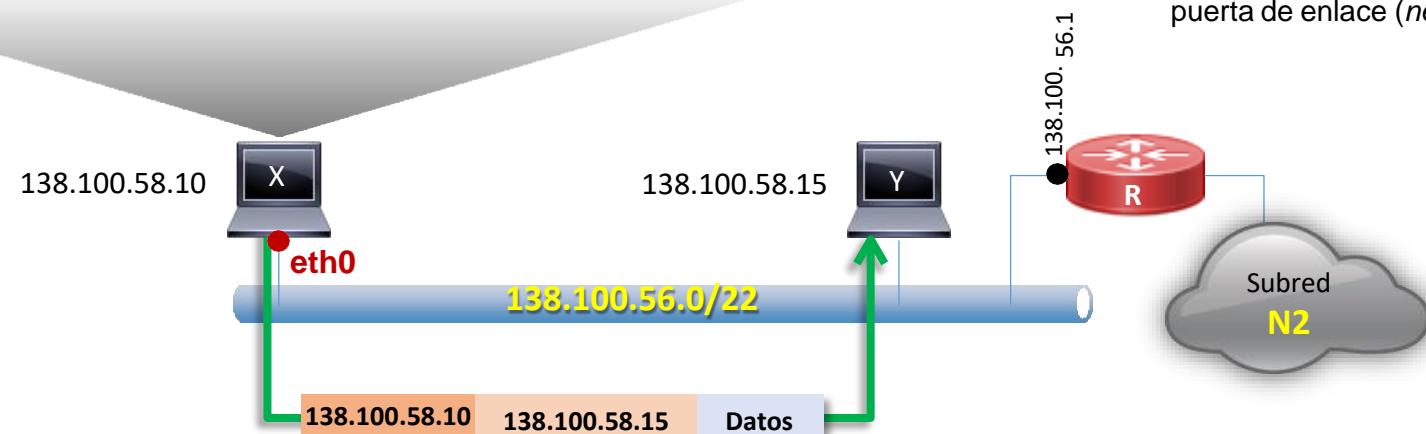
Tabla de rutas del host

Destino	Máscara	Gateway	Interface
138.100.56.0	255.255.252.0	*	eth0
Default	*	138.100.56.1	eth0

Siguiente salto (*next hop*) o puerta de enlace:
indica una dirección a la que el paquete debe ser
enviado para alcanzar su destino final

Campo adicional que indica
qué interfaz local lleva a la
puerta de enlace (*next hop*)

Entrada: **por defecto**

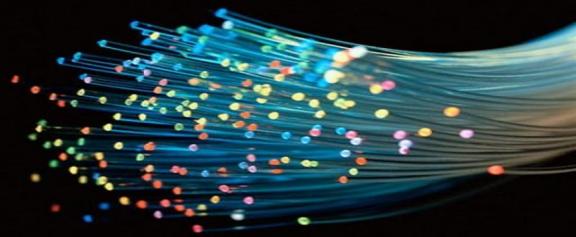


1. Esto se sabe gracias a la máscara

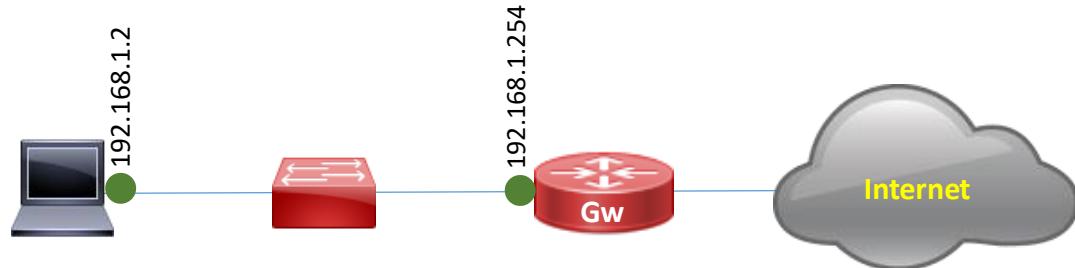
Eth0: es un identificador lógico

Tabla de rutas del host

Comando del sistema *netstat -r*



- La tabla de encaminamiento del host, es un documento electrónico que almacena las rutas a los diferentes nodos en una red informática
 - Se obtiene con el comando del sistema *netstat -r*



```
C:\> netstat -r
Route Table
=====
=====
Active Routes:
Network Destination      Netmask     Gateway       Interface   Metric
          0.0.0.0        0.0.0.0   192.168.1.254    192.168.1.2      20
         127.0.0.0      255.0.0.0    127.0.0.1    127.0.0.1       1
      192.168.1.0    255.255.255.0   192.168.1.2    192.168.1.2      20
<Output omitted>
```

El encaminamiento IP

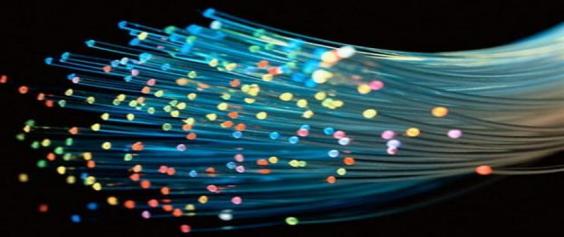
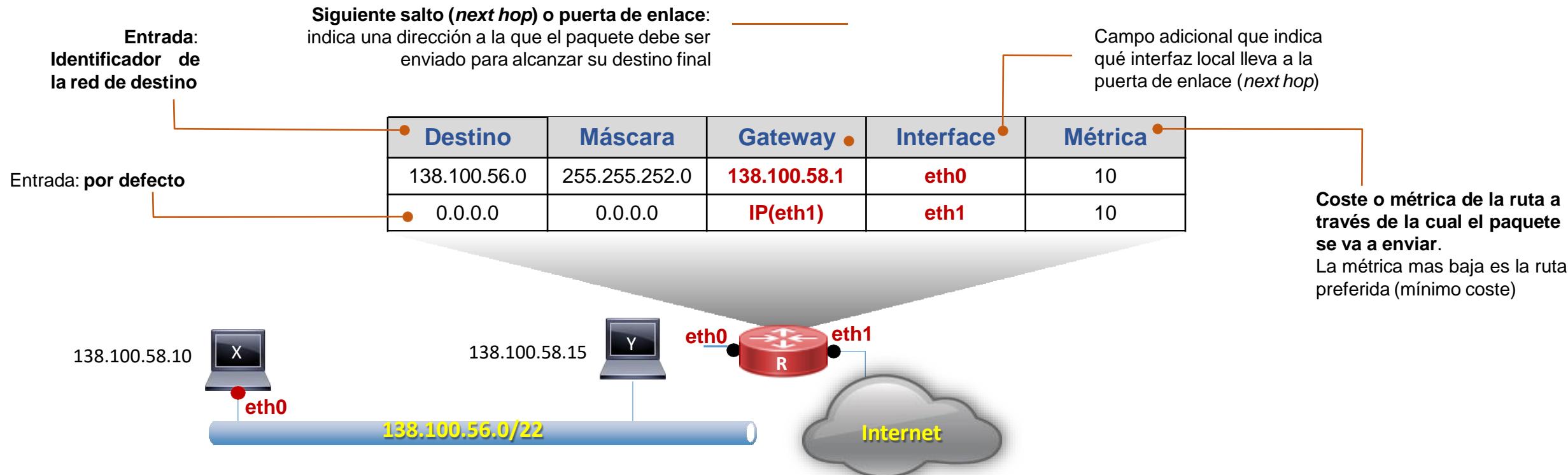


Tabla de encaminamiento del router [1]

■ Una tabla de encaminamiento es un archivo de datos, residente en la memoria RAM, que se utiliza para almacenar información de las rutas de redes conectadas directamente y de las remotas



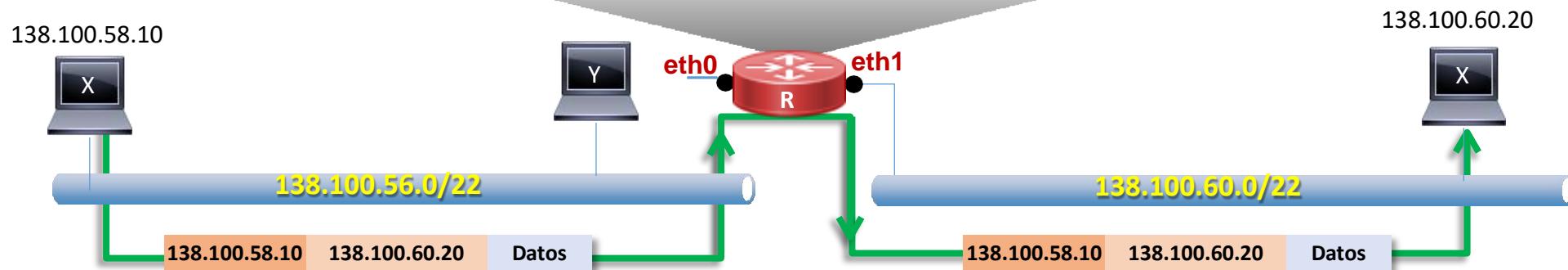
El encaminamiento IP



Tabla de encaminamiento del router [2]

- El host origen sabe que 138.100.60.20 no pertenece a su subred, por lo que manda el datagrama al router.
- En el router se consultan las tablas de encaminamiento que indican el siguiente salto (*next hop*) o puerta de enlace hacia la que hay que reenviar el datagrama

Destino	Máscara	Gateway	Interface	Métrica
138.100.56.0	255.255.252.0	138.100.56.1	eth0	10
138.100.60.0	255.255.252.0	138.100.60.1	eth1	10



4.6. Casos de estudio de encaminamiento



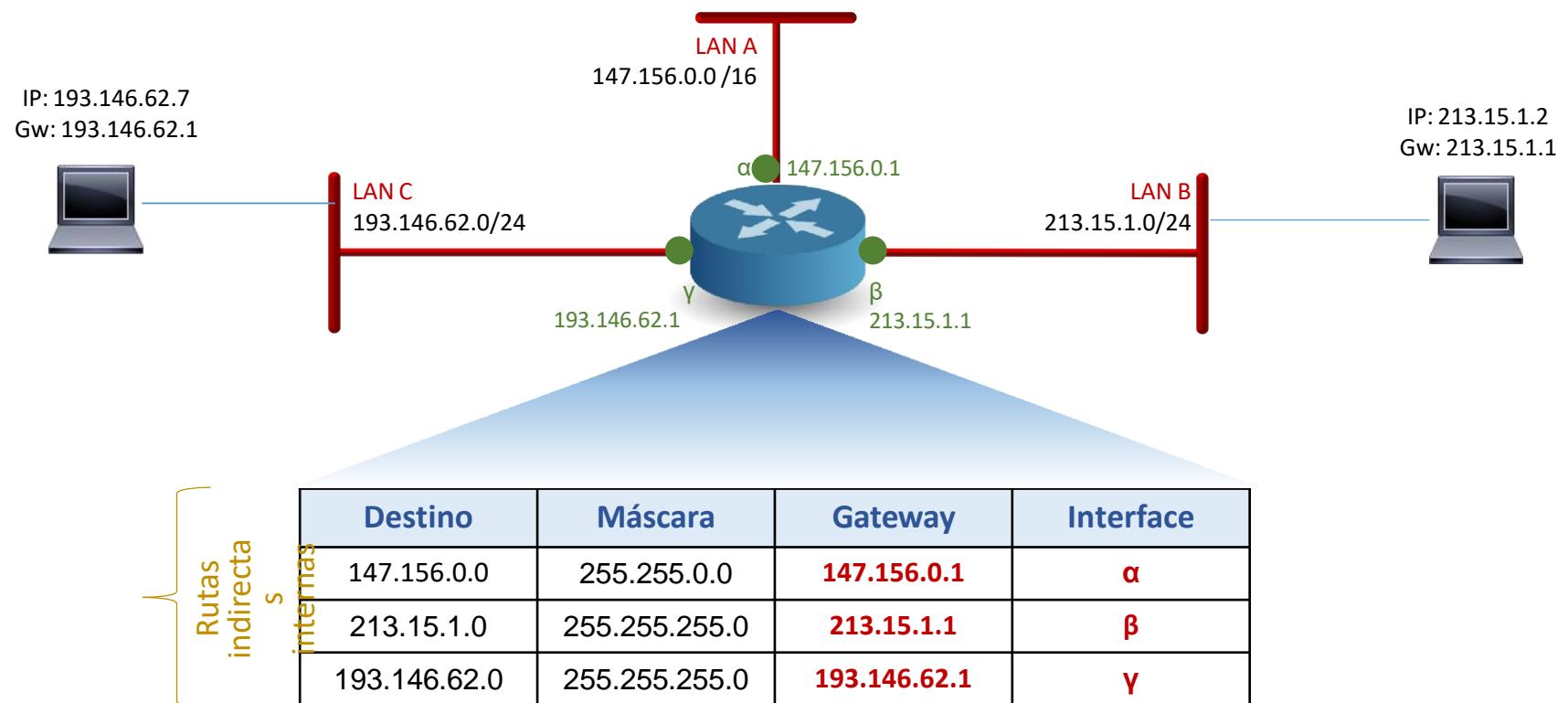
- LANs directamente conectadas
- LANs indirectamente conectadas
- LANs conectadas por una línea serie
- Encaminamiento en una topología en estrella
- Encaminamiento hacia Internet
- Conexión de un host a múltiples redes

Encaminamiento indirecto interno

LANs directamente conectadas

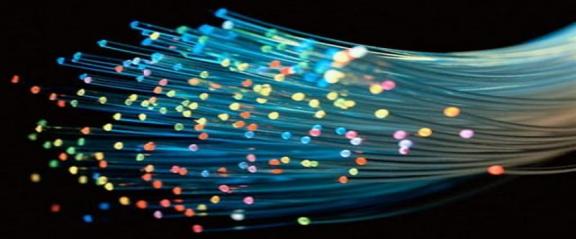


- El **encaminamiento indirecto interno** se produce cuando un router coge los datagramas de la red origen y los pone directamente (internamente) en la red de destino
 - El router está directamente conectado a tres LANs

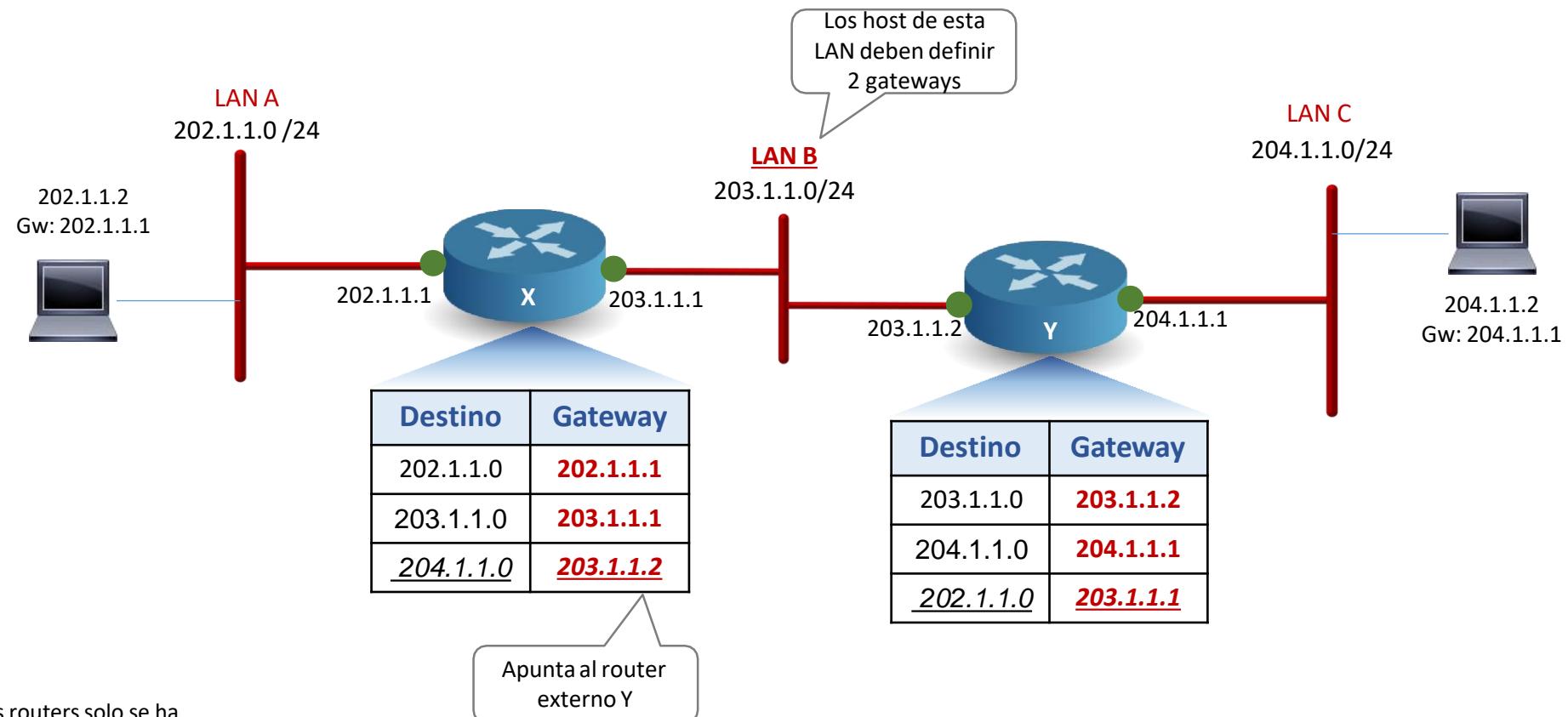


Encaminamiento indirecto externo

LANs indirectamente conectadas



- El **encaminamiento indirecto externo** se produce cuando un host quiere enviar datos a un host externo a las subredes que tiene directamente conectadas

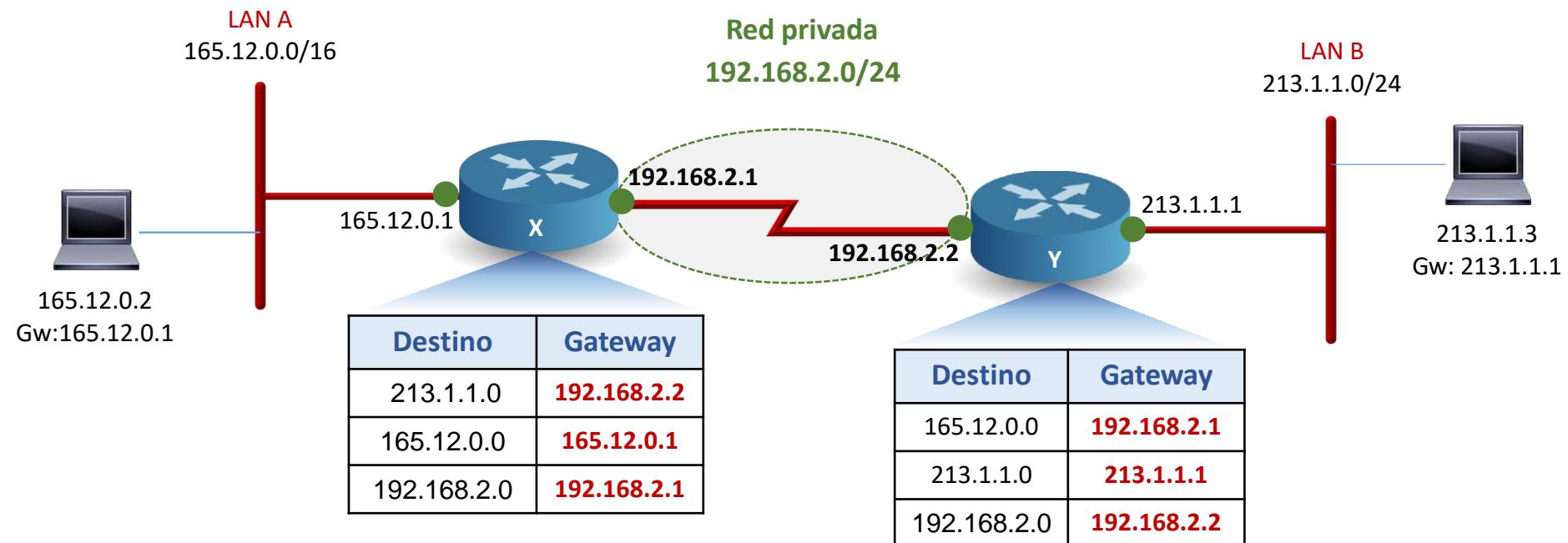


Nota: En la tablas de los routers solo se ha expresados las rutas indirectas externas

LANs conectadas por una línea serie



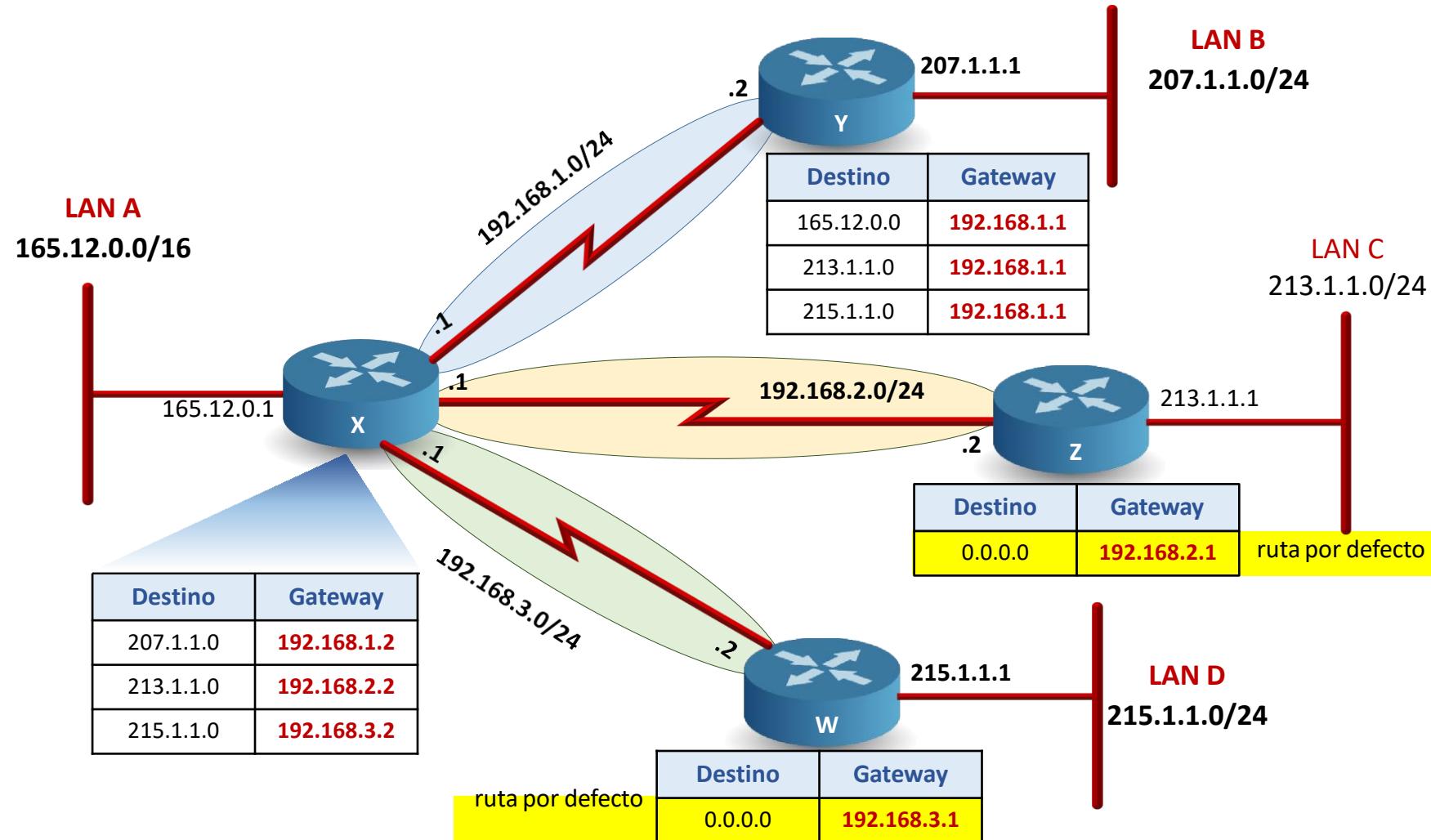
- Se asigna un direccionamiento privado para la línea serie
 - Dado que las interfaces serie no serán accedidas directamente por los usuarios normales es bastante frecuente utilizar en estos casos direcciones del rango privado según se especifica en el RFC 1918, para no desperdiciar direcciones públicas



Nota: En la tablas de los routers solo se ha expresados las rutas indirectas externas

Encaminamiento en una topología en estrella

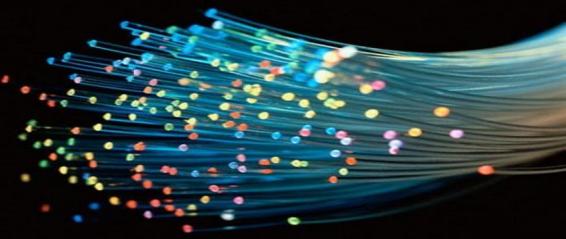
Rutas por defecto



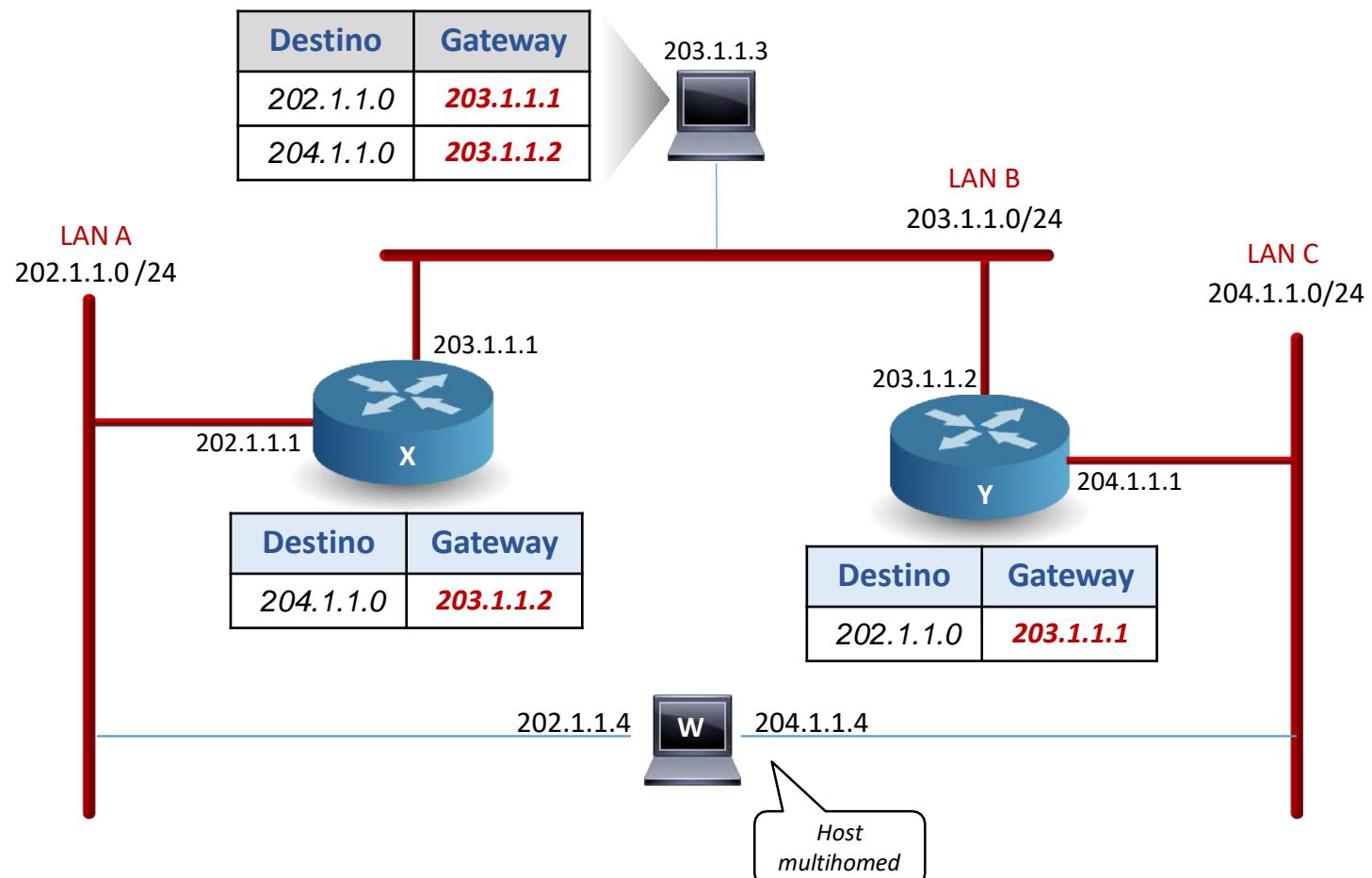
- La entrada por defecto evita que las tablas de los routers tengan que almacenar todas las redes de destino
 - Un router normalmente especifica las rutas más cercanas. El resto de rutas se indican mediante un gateway por defecto
 - Al gateway por defecto se le envían aquellos datagramas que no se saben encaminar

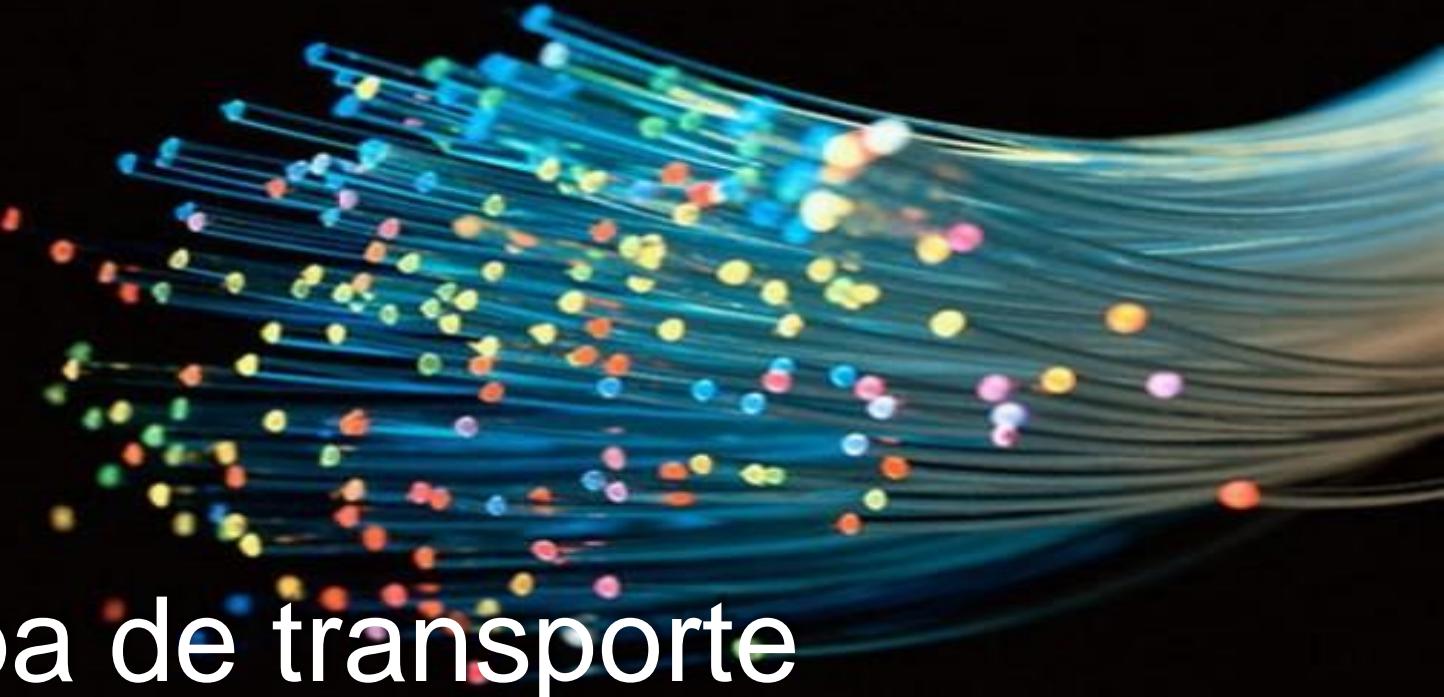
Nota: En la tablas de los routers solo se ha expresado las rutas indirectas externas

Conexión de un host a múltiples redes



- Para que un host pueda conectarse a múltiples redes necesita tantas interfaces de red como redes a las que quiera conectarse





5. La capa de transporte

Introducción

TCP vs. UDP

SAP de transporte y de red

El protocolo UDP. Encapsulado

Características

Los puertos *bien conocidos*

Formato del datagrama UDP

Transferencia de datos UDP

El protocolo TCP. Características

Formato del segmento TCP

Servicios de TCP

Establecimiento de la conexión TCP

Transferencia de datos

La capa de transporte

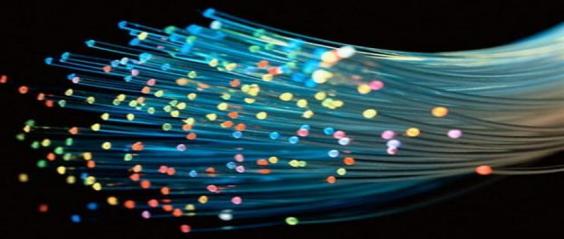
Introducción



- El protocolo de transporte provee la comunicación lógica entre programas/procesos de aplicación que se ejecutan en diferentes host
 - La información de transporte se transmite como una secuencia de **segmentos** (TCP) o **datagramas** (UDP) que se dirigen a la aplicación remota por el puerto especificado en la cabecera
 - La información generada por la capa de transporte (los datagramas IP) se encamina independientemente por la red: puede llegar a su destino por caminos diferentes y en diferente orden en al que se generaron. En recepción, todos los elementos de información (los datagramas IP) se reordenan para reconstruir la información de transporte (segmentos o datagramas UDP)



TCP vs. UDP



TCP

Protocolo orientado a conexiones

Mas lento pero confiable

Control de flujo

Reconocimiento/
retransmisiones

Desde pequeñas a grandes
cantidades de datos

UDP

Protocolo sin conexiones

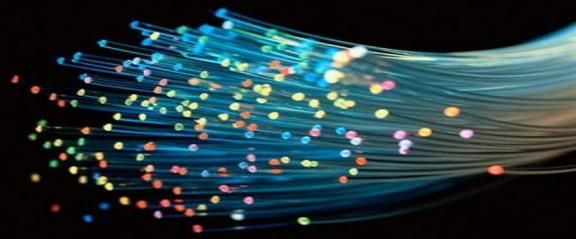
Mas rápido pero sin garantía
(*best effort*)

Sin control de flujo

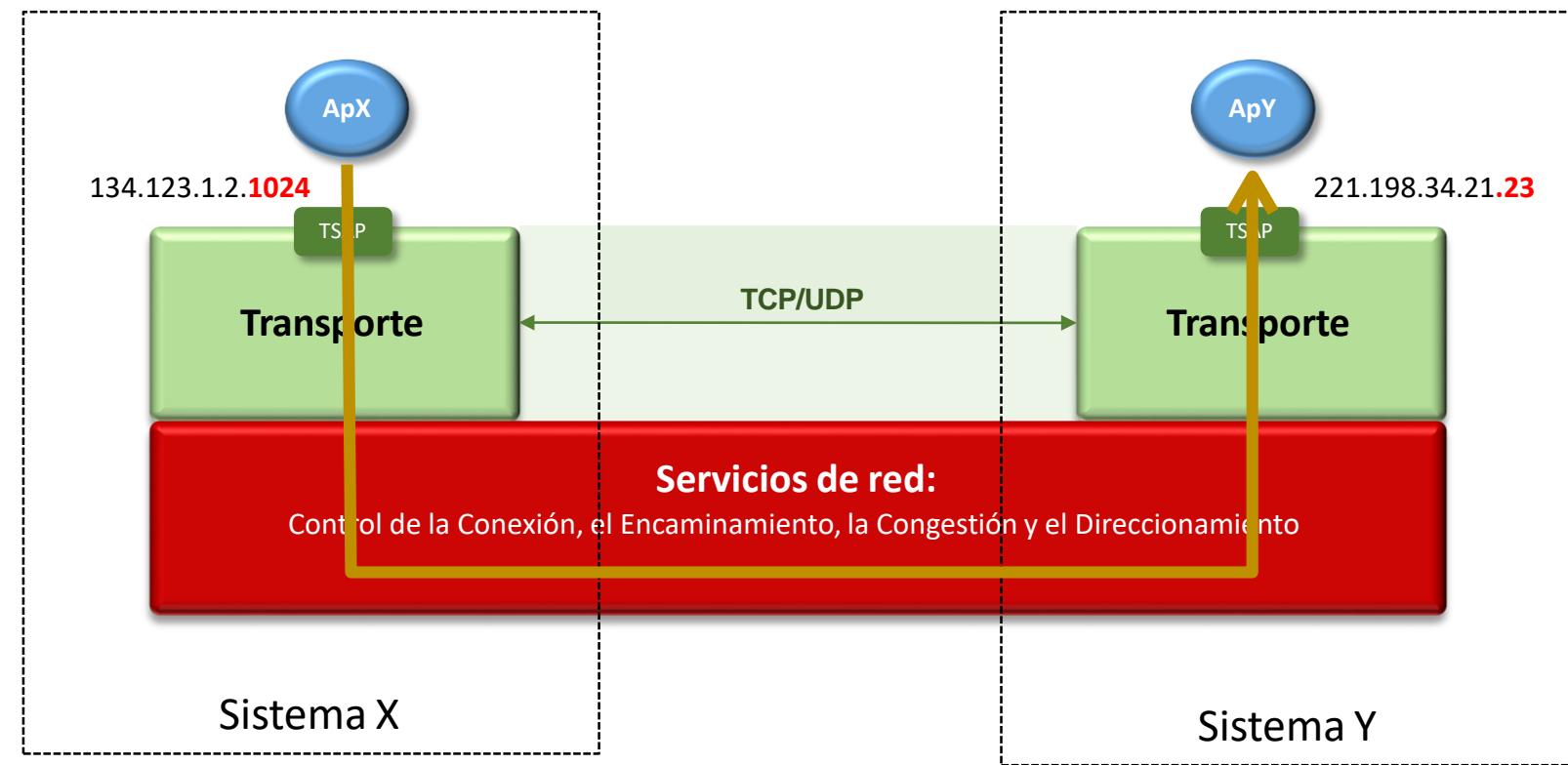
Sin reconocimiento

Pequeñas cantidades de datos

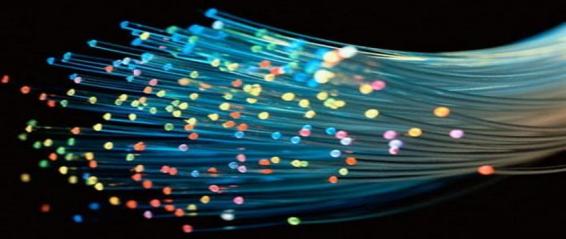
Los puertos



- El nivel de transporte ofrece sus servicios al nivel de aplicación a través de unos SAPs específicos denominados *ports* o **puertos**
 - Cada puerto del Nivel de Transporte ofrece a las aplicaciones un interfaz de acceso a la red de comunicaciones, permitiéndole dialogar con otra aplicación situada en otro puerto en una máquina remota



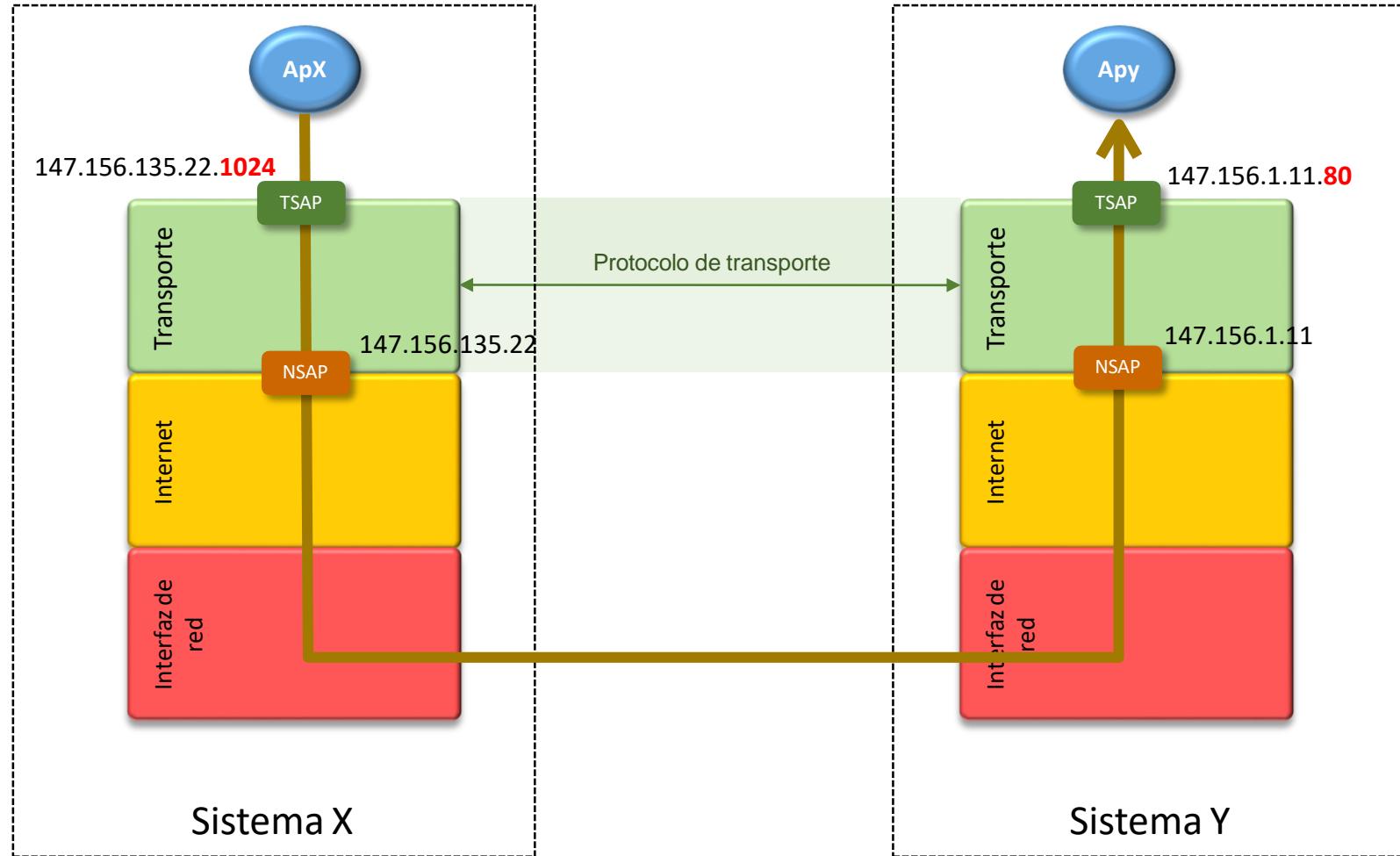
Los puertos *bien conocidos*



- Los puertos < 1024 conocidos como “puertos bien conocidos” (*well-known ports*) están reservados para servicios estandarizados. Están descritos en el RFC 1700: *Assigned Internet Numbers*
 - El resto de los puertos está disponible para aplicaciones de usuario de forma temporal, pero también pueden representar servicios que hayan sido registrados por un tercero (rango de puertos registrados: 1024 al 49151).

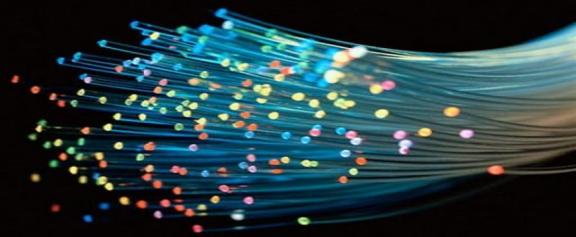
Puertos UDP	Puertos TCP
0 Reservado	0 Reservado
7 ECHO	20 FTP-DATA
13 DAYTIME	21 FTP (control)
37 TIME	23 TELNET
42 NAMESERVER	25 SMTP
53 DOMAIN	42 NAMESERVER
69 TFTP	53 DOMAIN
	80 HTTP
	995 POP3 sobre SSL

Puntos de acceso al servicio de transporte y de red TSAP y NSAP

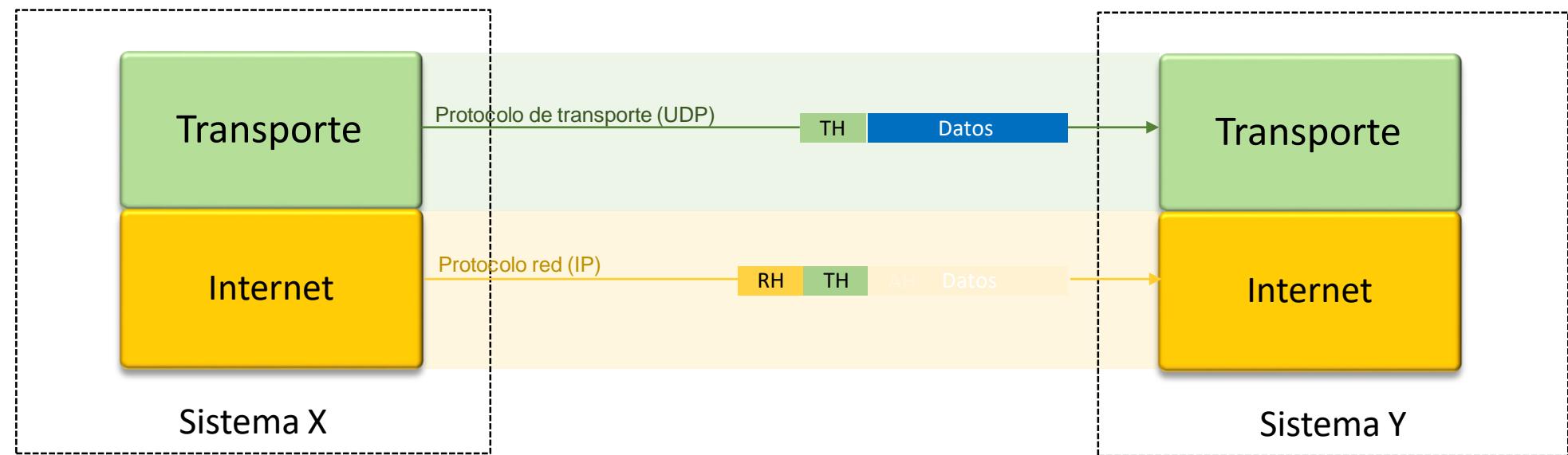


El protocolo UDP

Encapsulado

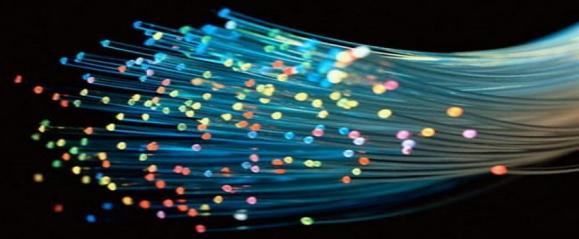


- El protocolo de datagrama de usuario (*User Datagram Protocol*), especificado en el RFC 768, proporciona un servicio no orientado a conexión para los procedimientos de la capa de aplicación



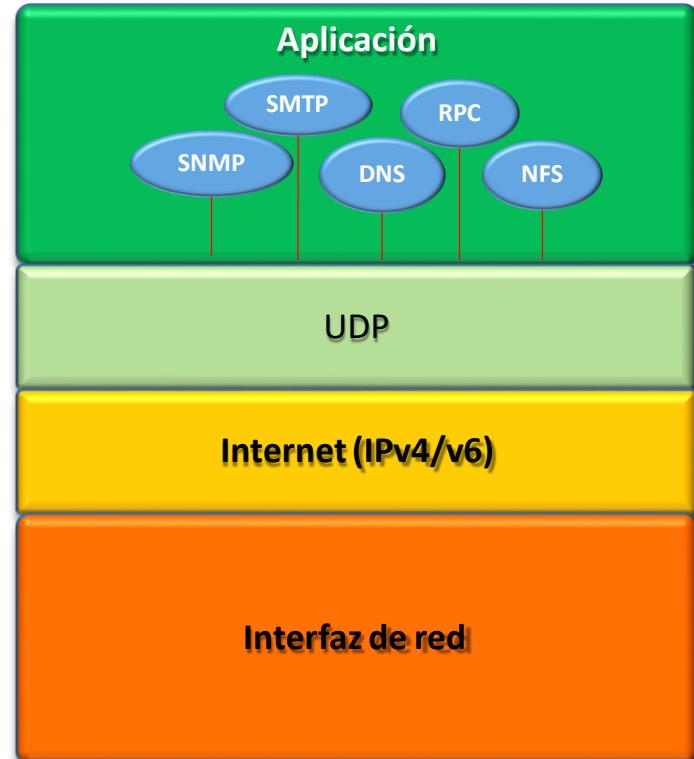
El protocolo UDP

Características



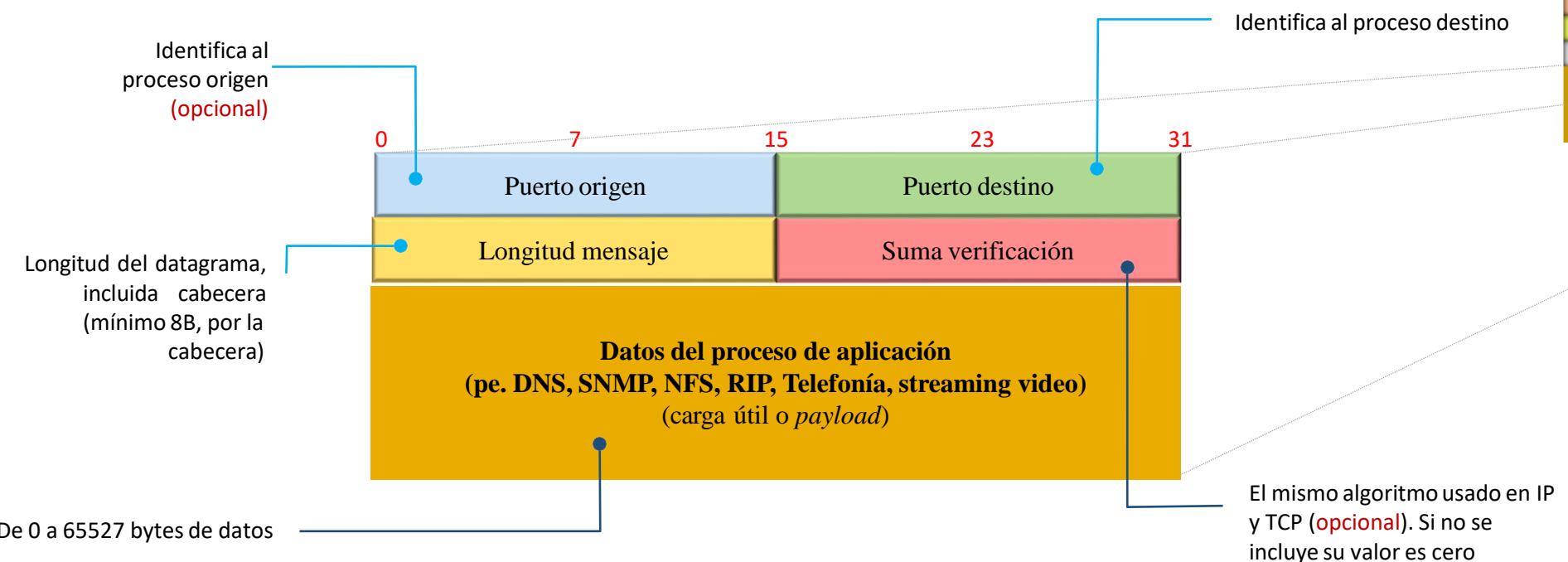
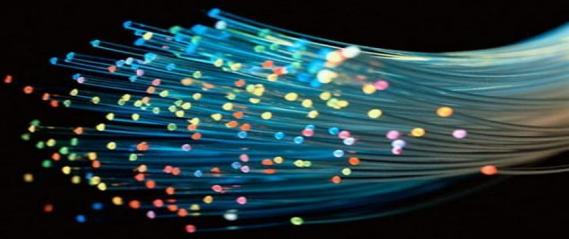
Servicio sencillo, CLNS, no fiable

- No necesita preestablecer la comunicación antes de enviar los datos
- La transmisión puede ser P2P y MP¹
- No dispone de mecanismos capaces de recuperar errores, garantizar la entrega, controlar el flujo, conservar el orden secuencial, ...
- No mantiene un control sobre el tráfico enviado o recibido por lo que no hay retransmisión del datagrama UDP
- La comunicación **se compone sólo de los mensajes de datos**. No hay mensajes de control para detener una aplicación

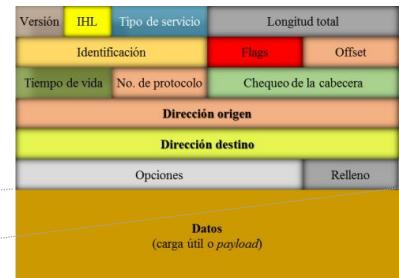


TFTP (*Trivial File Transfer Protocol*): protocolo sencillo de transferencia de ficheros.
DNS (*Domain Name Server*): para la resolución de nombres.
SNMP (*Simple Network Management Protocol*): protocolo de gestión de red

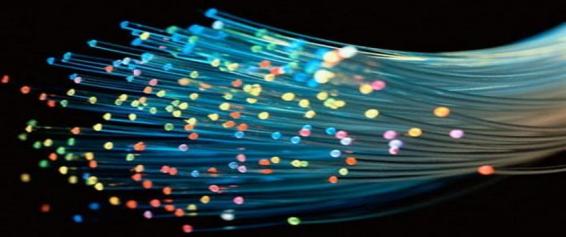
Formato del datagrama UDP



Datagrama IP

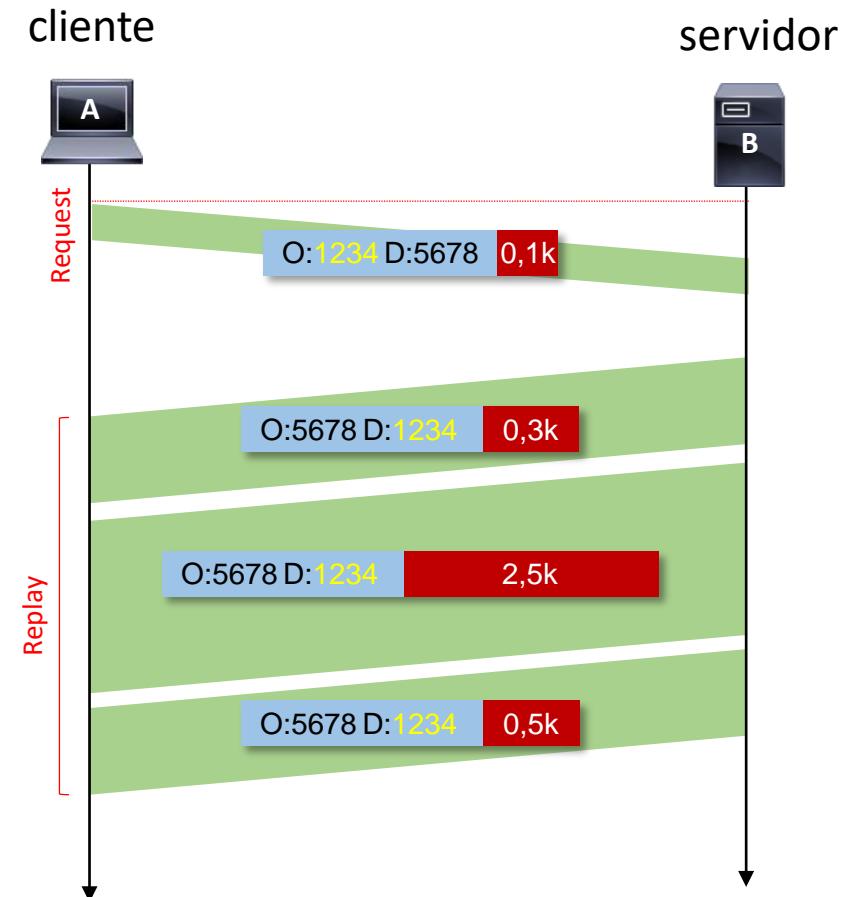


Transferencia de datos UDP



■ La transferencia de datos en UDP es simplemente una extensión del servicio de datagramas IP

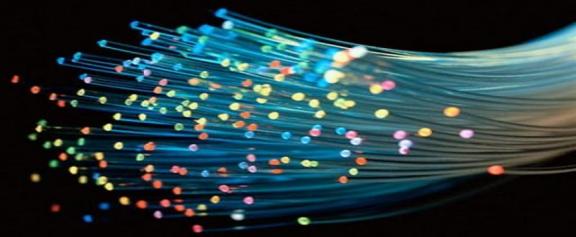
- En UDP ni el cliente establece una conexión con el servidor, simplemente envía un datagrama al servidor usando la llamada al sistema, ni el servidor tiene que aceptarla.
- El servidor simplemente emite una llamada al sistema para recibir datos, y a continuación, espera hasta que llegan los datos de algún cliente.
- En UDP no existe una secuencia de datos. La entrega de los datos no se puede garantizar y no existe una retransmisión de paquetes perdidos.
- UDP añade multiplexación al servicio de los datagramas mediante los puertos
- Los mensajes que envía la aplicación se mapean 1:1 en datagramas UDP y estos en datagramas IP



O: puerto origen
D: puerto destino

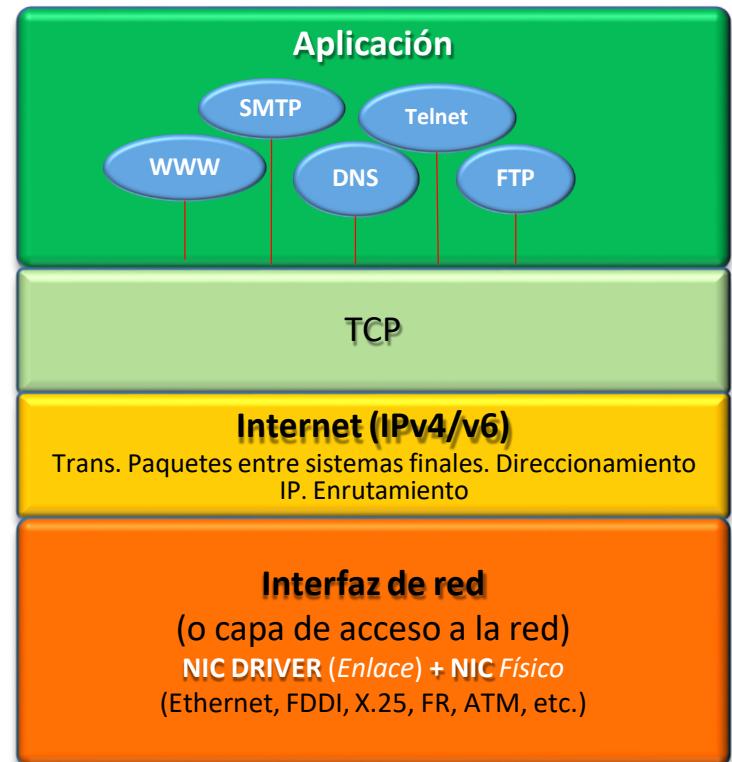
El protocolo TCP

Características

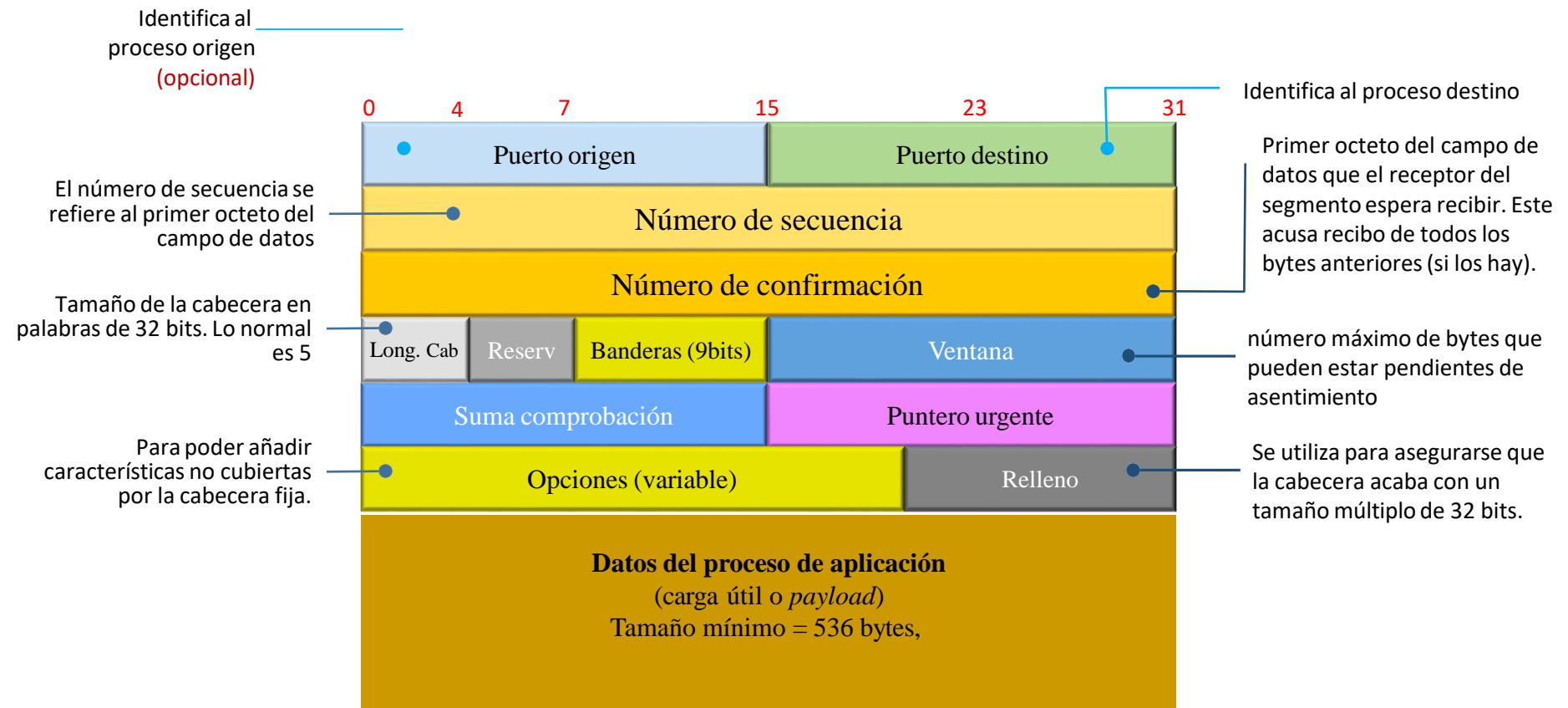
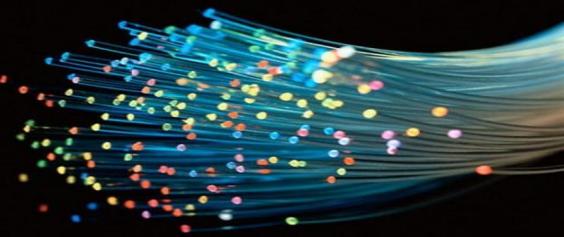


■ El protocolo TCP ofrece un servicio orientado a conexión y fiable entre pares de procesos

- La conexión es *Full Duplex* y P2P
- La transferencia se apoya en el envío continuo con buffers para almacenamiento de segmentos pendientes de asentimiento.
- TCP proporciona control de flujo mediante esos buffers.
- Los datos de la aplicación son troceados y se integran en PDUs llamadas **segmentos**.
- Al transmitir cada segmento se espera un asentimiento. Si no llega en un determinado plazo, se retransmite el segmento.
- Si el receptor recoge un segmento con checksum inválido, lo rechaza y no envía el asentimiento.
- Los segmentos TCP se reordenan en recepción, pasándose en orden a la aplicación.
- TCP descarta los duplicados en recepción y se recupera de las pérdidas.



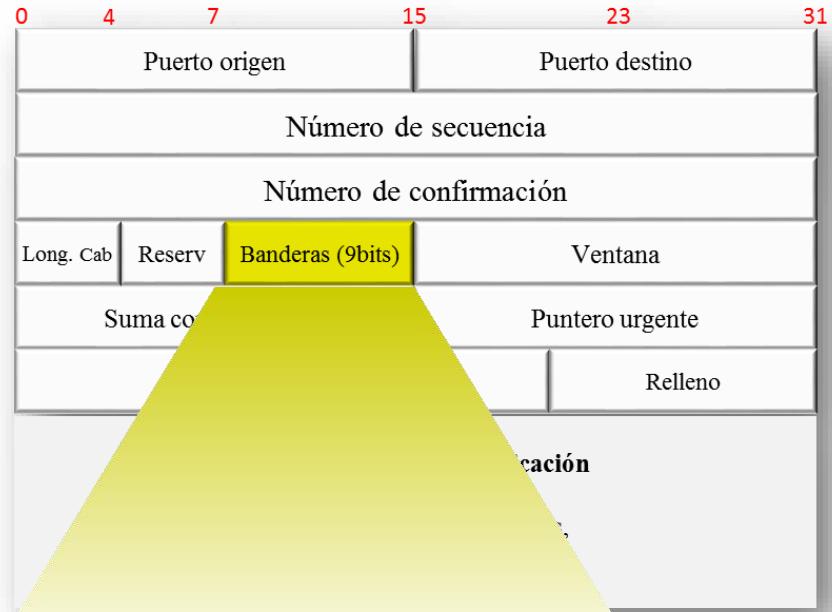
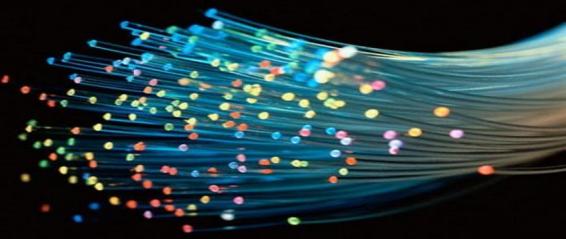
Formato del segmento TCP



¡Un segmento TCP siempre se transporta en un datagrama IP!

Formato del segmento TCP

Banderas (Flags)



Indica si el campo de puntero a datos urgentes es válido

URG

ACK

PSH

RST

SYN

FIN

Número de asentimiento es válido.

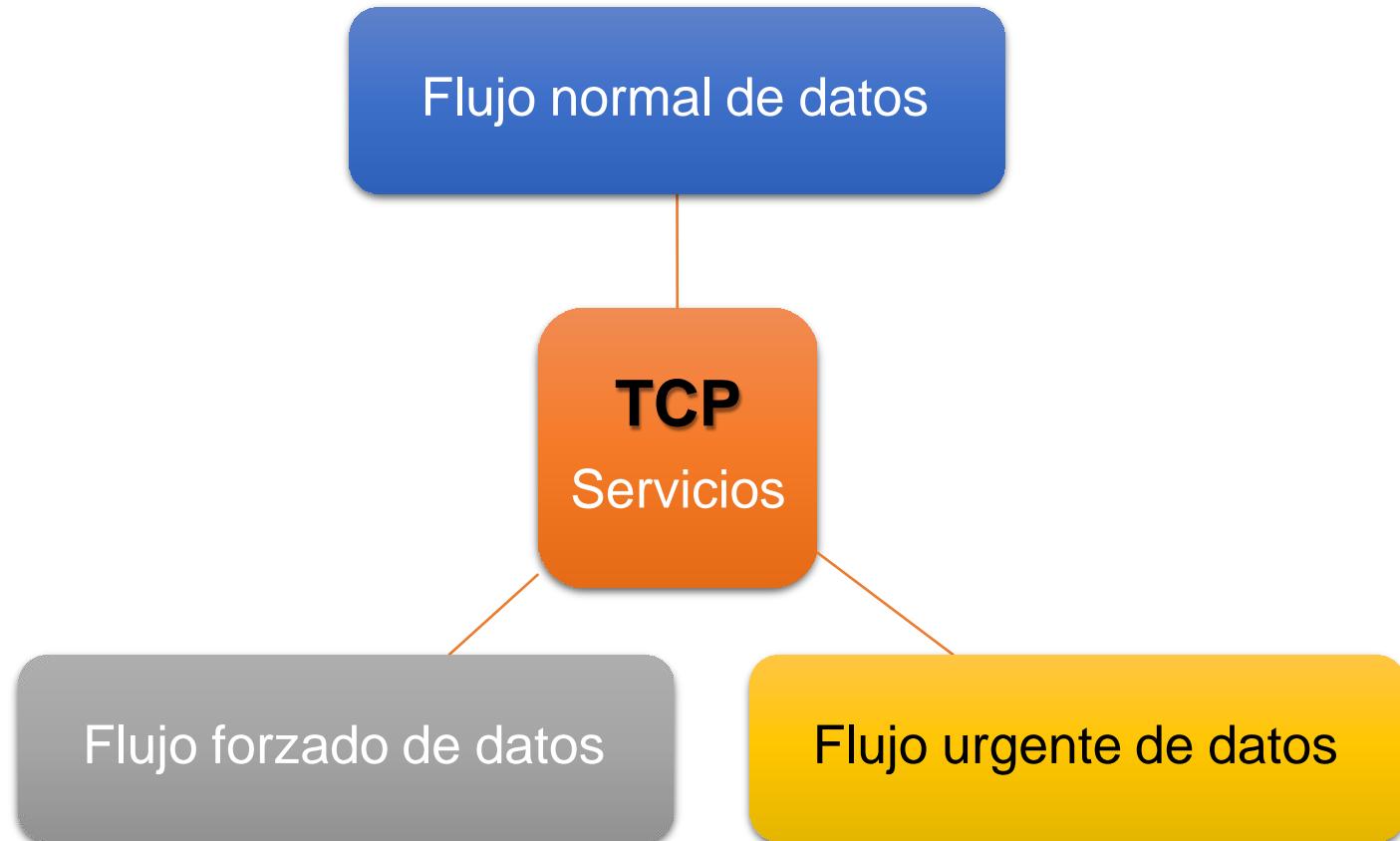
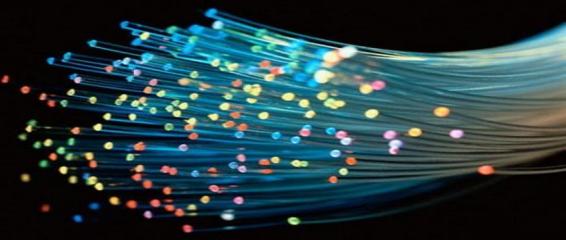
El receptor debe pasar los datos a la aplicación tan pronto como sea posible.

El emisor finaliza el envío de datos

Sincroniza los números de secuencia para iniciar la conexión

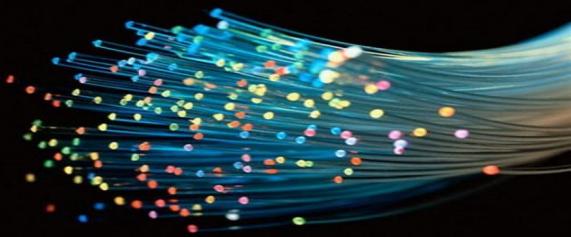
Cortar/reinicializar la conexión.

Servicios de TCP

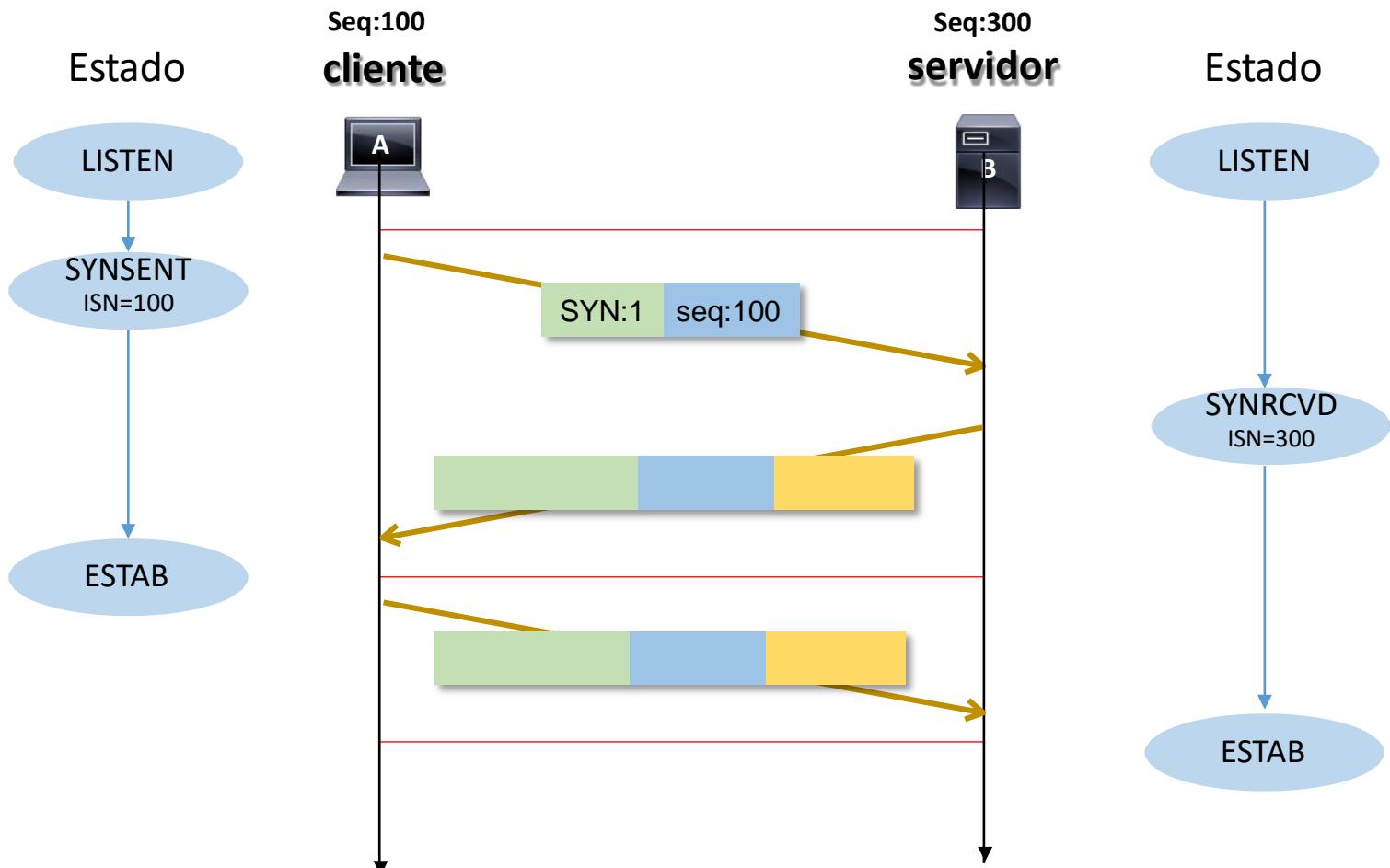


Establecimiento de la conexión TCP

Conexión en tres fases

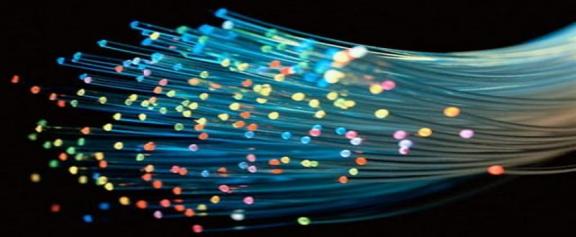


- El **Three Way Handshake** - saludo a tres vías - es un procedimiento de conexión que evita los problemas debidos a duplicados
 - 1) El cliente inicia el establecimiento de una conexión activando el flag **SYN**. El número de secuencia (**seq**) no empieza normalmente en 0, sino en un valor denominado ISN (*Initial Sequence Number*) elegido al azar
El ISN sirve de 'PIN' en el saludo a tres vías para asegurar la autenticidad de la comunicación. Supongamos que $ISN=100$
 - 2) El servidor responde con un mensaje en el que acusa recibo de la petición y le indica al cliente qué número **seq** ha elegido él para la comunicación en sentido inverso. En este caso es 300
 - 3) El cliente envía un tercer mensaje (Número de secuencia $seq=100+1$) en el que acusa recibo del segundo ($ack=300+1$) y considera establecida la conexión. Cuando recibe este tercer mensaje el servidor considera establecida la conexión
 - 4) Todos los paquetes después del SYN tienen activo el flag ACK



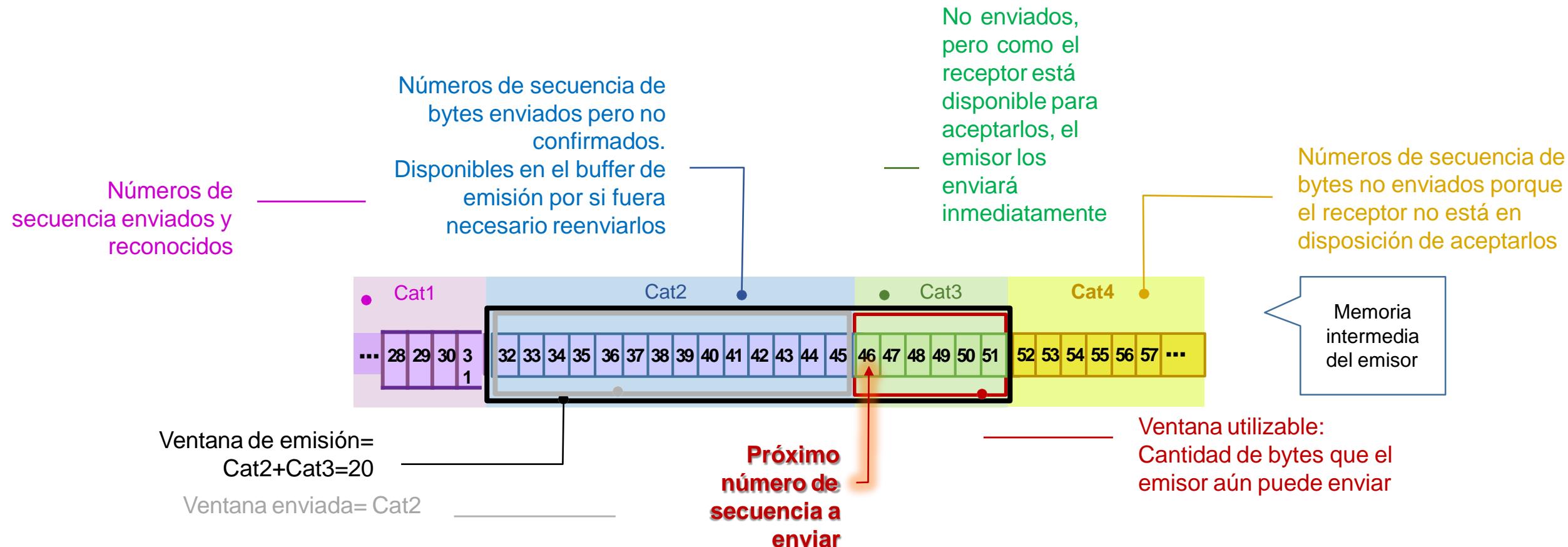
Transferencia de datos

Control de flujo mediante ventana



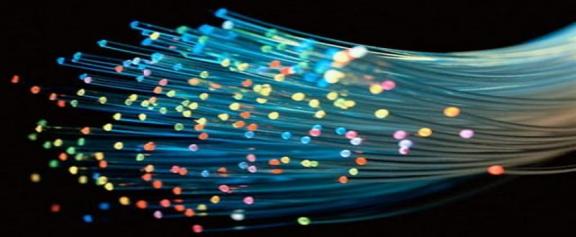
■ Cuando el servicio de red no es fiable se requiere control de flujo

- La técnica conocida como **ventana deslizante** permite a TCP mantener, cuidadosamente, un registro de los datos que envía y de lo que le sucede



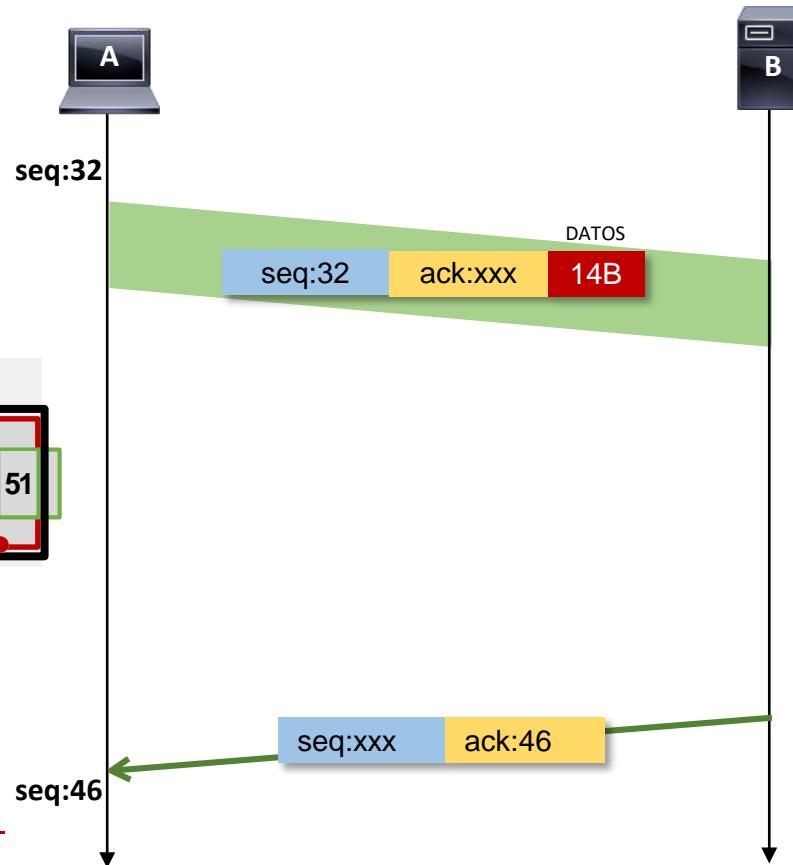
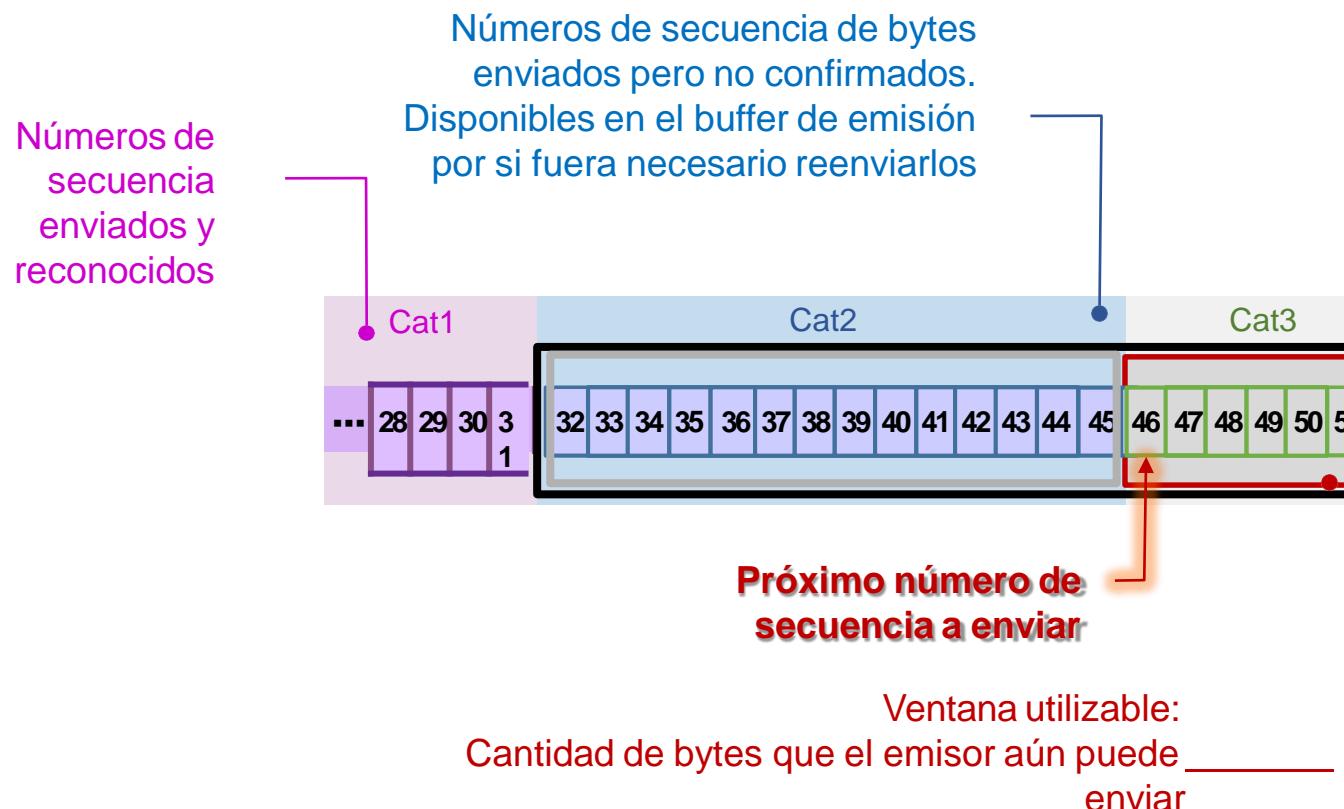
Transferencia de datos

Números de secuencia



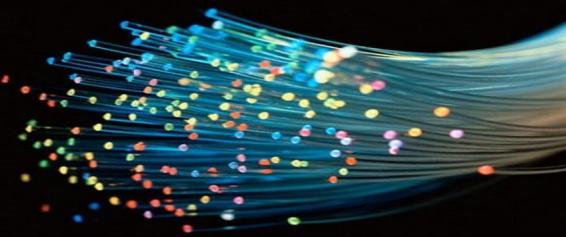
- El cliente TCP, a cada lado de una sesión TCP, mantiene un número de secuencia que utiliza para realizar un seguimiento de la cantidad de datos que ha enviado.

- Este número de secuencia se incluye en cada paquete transmitido, y es reconocido por el host contrario como un número de confirmación para informar al host remitente de que los datos transmitidos se han recibido correctamente.



Transferencia de datos

Números de secuencia. Caso de estudio: HTTP



Segmento # 4

- Este segmento lleva una solicitud HTTP (725B). El número es 1, ya que no hay datos. El número de reconocimiento también es 1, ya que tampoco se han recibido datos desde el servidor.

Segmento # 5

- El Segmento es enviado desde el servidor exclusivamente para reconocer los datos enviados por el cliente en el paquete # 4. Mientras las capas superiores procesan la petición HTTP. Observe que el número de acuse de recibo se ha incrementado en 725 (la longitud de la carga útil en el paquete # 4) a 726. El número de secuencia del servidor permanece en 1.

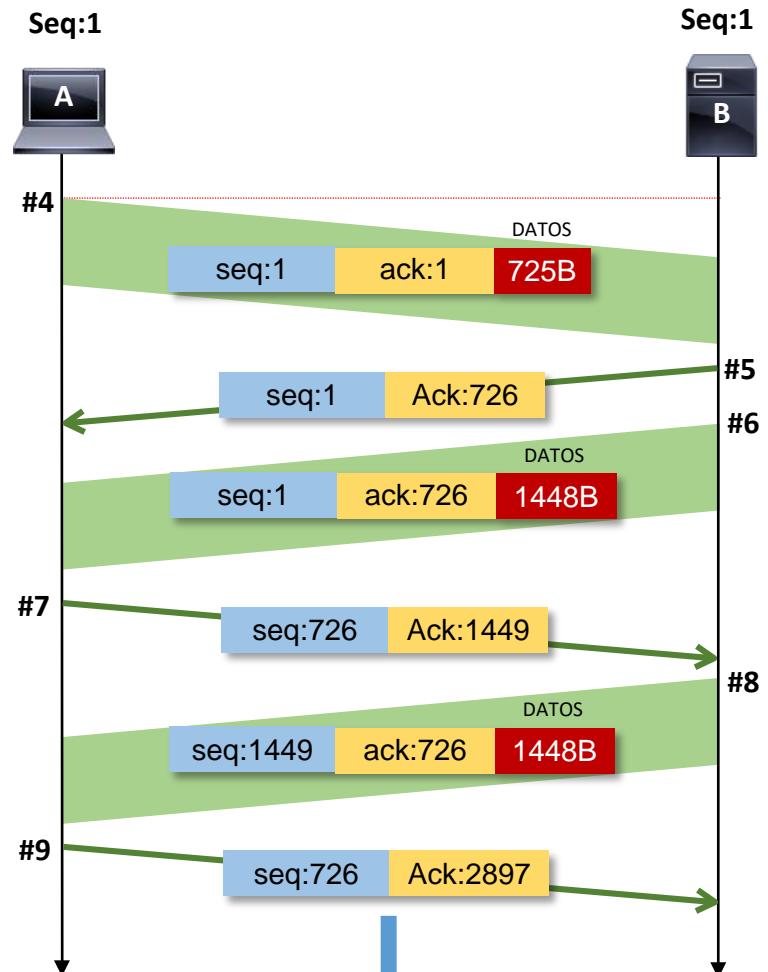
Segmento # 6

- Este segmento marca el inicio de la respuesta HTTP del servidor. Su número de secuencia es igual: 1, ya que ninguno de sus paquetes anteriores a éste han llevado a una carga útil. Sin embargo, este segmento lleva una carga útil de 1.448 bytes.

Segmento # 7

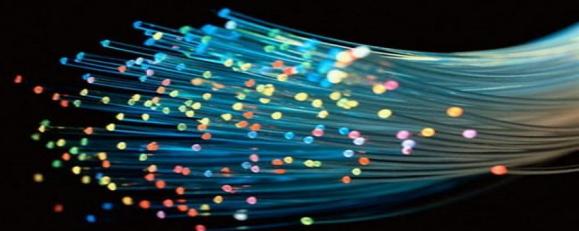
- El número de secuencia del cliente se ha aumentado a 726 por el último segmento que envió y que ya se confirmó. Habiendo recibido 1448 bytes de datos desde el servidor, el cliente aumenta su número de reconocimiento a 1.449.

El ciclo se repite. El número de secuencia del cliente se mantendrá estable en 726, ya que no tiene datos para transmitir más allá de la petición inicial de 725 bytes. En cambio, el número de secuencia del servidor continuará creciendo ya que envía más segmentos de la respuesta HTTP.

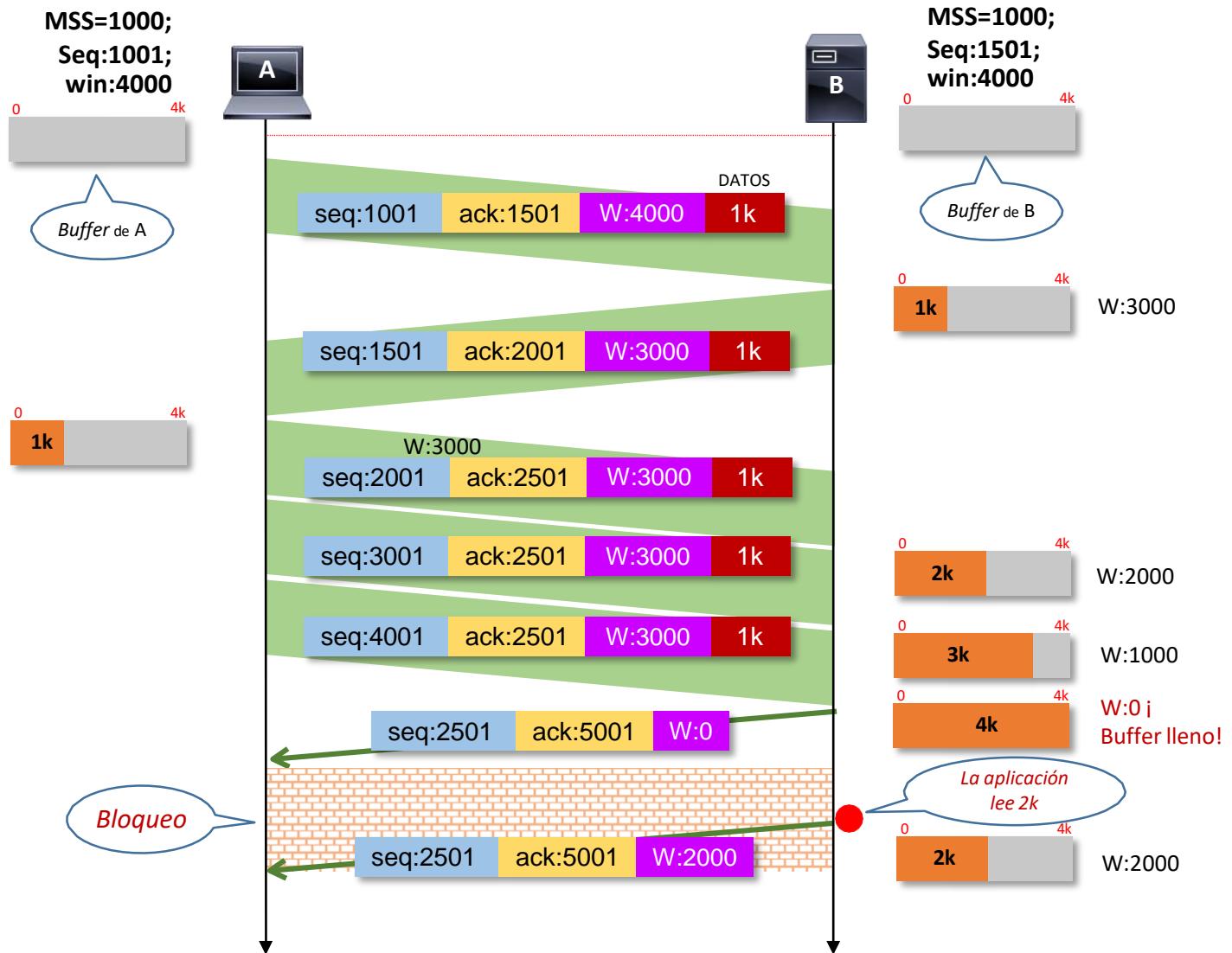


Transferencia de datos

Control de flujo mediante ventana. Un caso de estudio



- El TCP receptor devuelve al TCP emisor, con cada ACK, una **ventana**, en la que "anuncia" el rango de números de secuencia aceptables más allá del último segmento recibido con éxito.
- Esta **ventana** especifica el número de octetos, a contar a partir del número del acuse de recibo, que el TCP emisor de la ventana (el receptor de los datos) está en ese momento preparado para recibir y, consecuentemente, que se permite que el emisor transmita antes de que reciba el siguiente permiso.
- El sistema remitente no puede enviar un número de bytes superior al espacio disponible en el **buffer** de recepción del sistema receptor
- Una vez que la aplicación receptora drena los datos del buffer de recepción, el sistema receptor podrá responder con un tamaño de ventana igual a la cantidad de datos leídos. A continuación, el TCP de sistema remitente podrá reanudar el envío de datos.

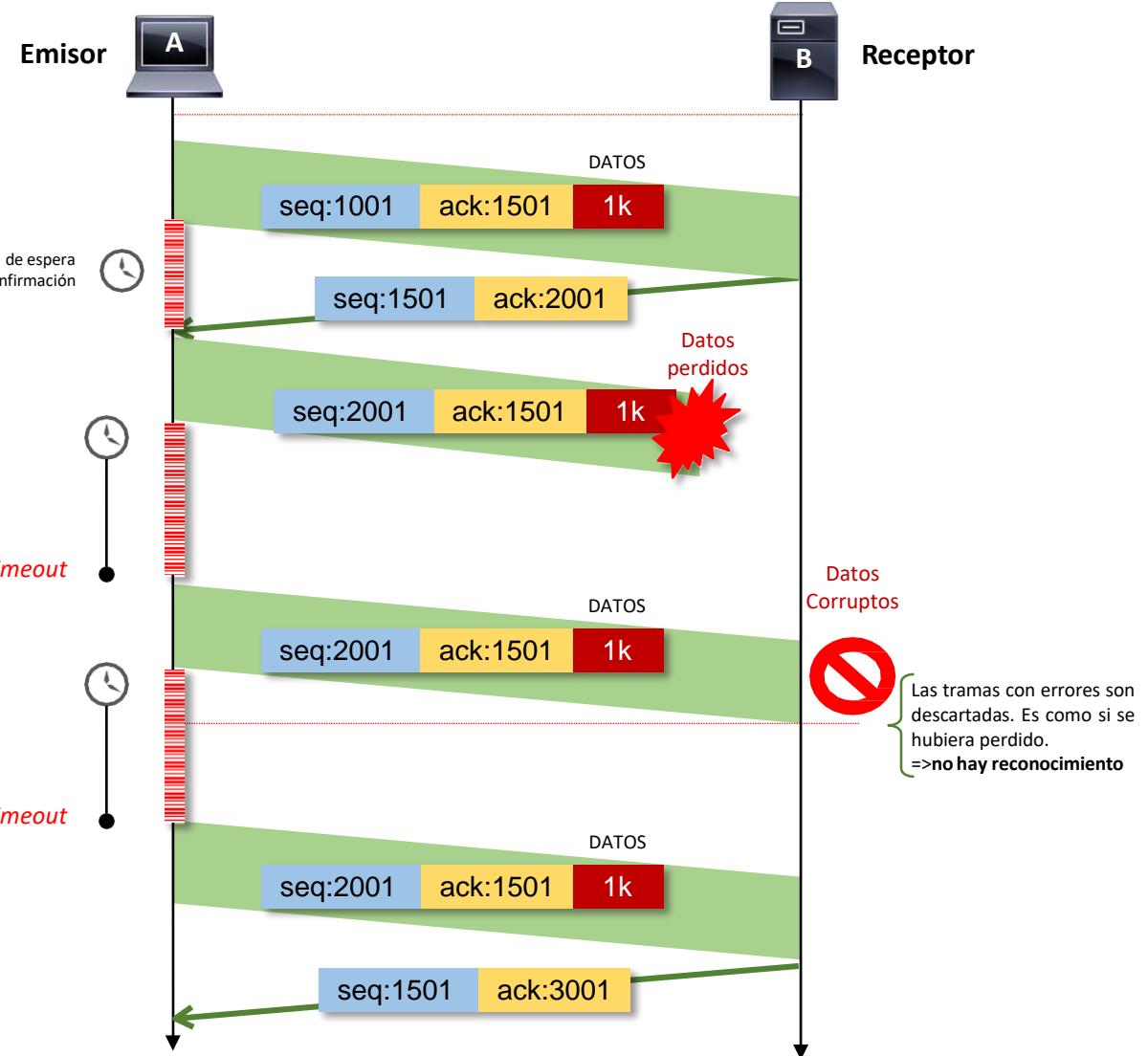


Transferencia de datos

Pérdida de segmentos. Retransmisiones

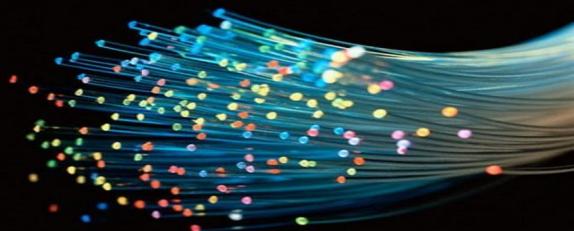


- Los errores (tramas dañadas y tramas perdidas), una vez detectados, se recuperan con retransmisiones
 - Cada vez que envía un segmento, el software TCP inicia un temporizador y espera por un acuse de recibo.
 - El ACK no llegará al emisor:
 - Si se pierde el segmento de datos.
 - Se pierde el ACK correspondiente.
 - El checksum no es correcto (se descarta el segmento y se actúa como si se hubiera perdido).
 - En cualquiera de los casos, expirado el temporizador se retransmite el segmento asignado al temporizador consumido.



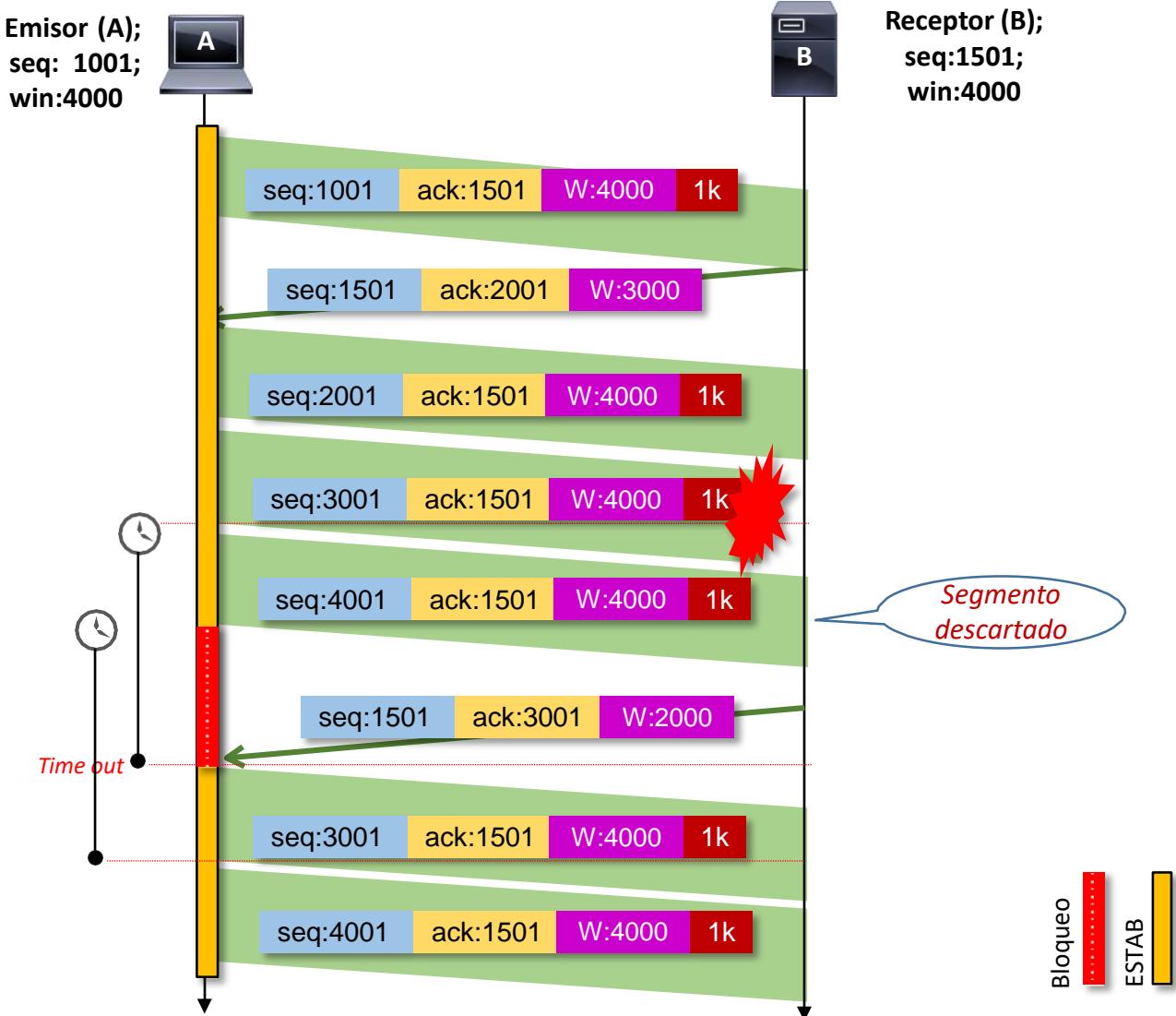
Transferencia de datos

Pérdida de segmentos. Retroceso n



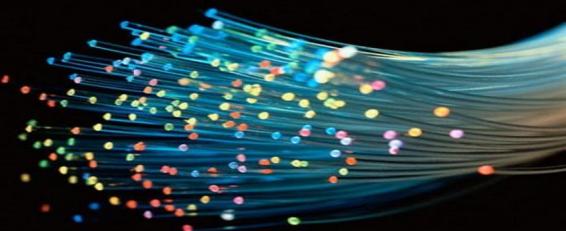
■ Si se enviaron varios segmentos y se pierde uno se puede hacer dos cosas:

- **Retroceso n** : Una vez agotado el temporizador, el emisor retransmite todos los segmentos que se encontraban en el buffer del transmisor a espera de validación, tanto el segmento perdido como los segmentos enviados posteriormente
- El remitente solo tiene que retransmitir los segmentos que han sido perdidos



Transferencia de datos

Flujo forzado de datos



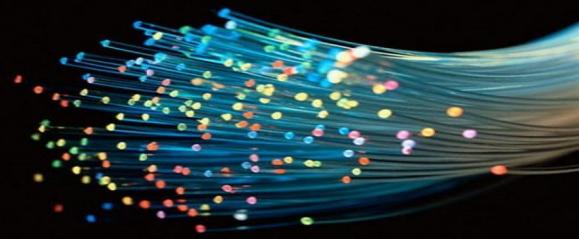
■ La activación del flag PSH, permite a la aplicación obligar a la entidad TCP emisora a crear inmediatamente un segmento, para llevar su PDU, y a enviarlo. Por su parte, la entidad TCP receptora los pondrá a disposición de la aplicación de inmediato.

- Para ello, los datos se envían sin esperar a llenar un segmento
- En la figura: A envía 3 segmentos con 1k de datos y con el flag PSH activado



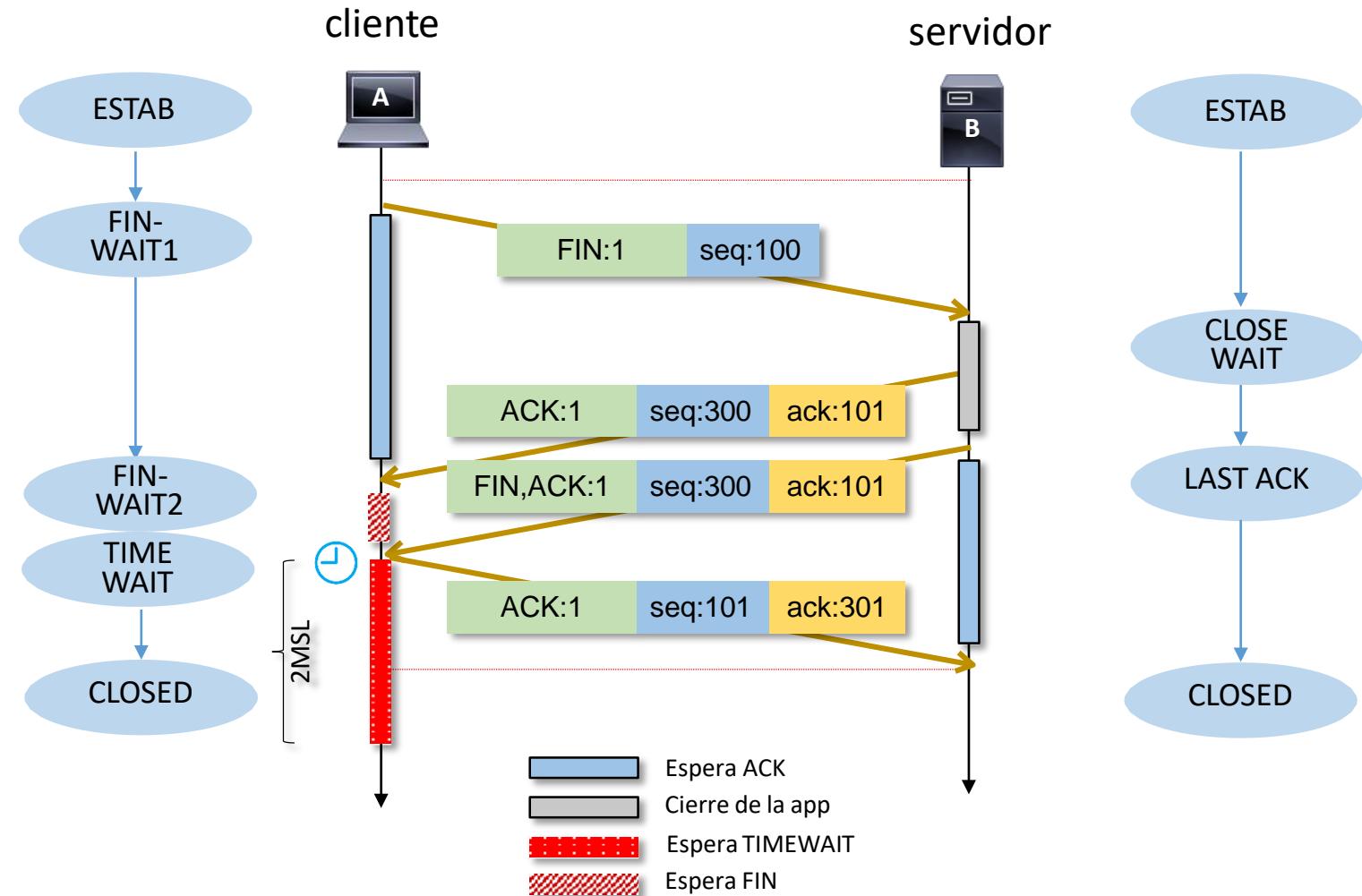
Fin de la conexión TCP

Desconexión simétrica en cuatro fases



- En la terminación simétrica cada host corta la conexión únicamente en el sentido en el que emite datos

- 1) El cliente, después de haber enviado un FIN, está esperando LA CONFIRMACIÓN . En este estado, el cliente todavía puede recibir datos desde el servidor, pero ya no aceptará los datos de su aplicación local que se envían al servidor
- 2) El servidor recibe del cliente FIN . Se envía un ACK para reconocer el FIN . El servidor debe esperar a que la aplicación de usarlo se cierre, por lo que la aplicación aquí puede demorarse para terminar lo que está haciendo
- 3) La confirmación ha llegado y el cliente está esperando el FIN del servidor. En este punto el servidor aún puede mandar datos. El cliente está esperando por el FIN del servidor
- 4) El servidor envía su FIN al cliente. El número de secuencia no cambia porque no ha habido reconocimiento
- 5) El cliente espera un período de tiempo igual al doble del tiempo máximo de vida del segmento (Máximo segment life, MSL), después de enviar el ACK





6. La capa de aplicación

Introducción

Modelo C/S vs. P2P

El modelo C/S

El protocolo de transferencia de archivos

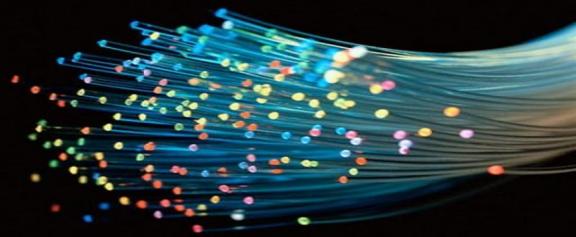
El sistema de nombres de dominio

Jerarquía DNS

Funcionamiento de DNS

La capa de aplicación

Introducción

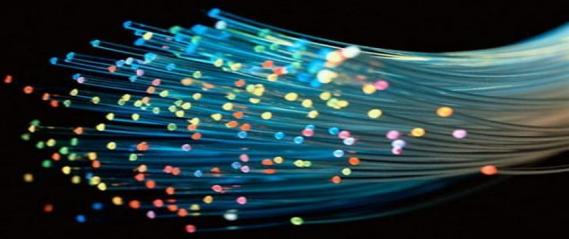


En el modelo TCP / IP, la capa de aplicación contiene los **protocolos de aplicación** y los **métodos** utilizados en las comunicaciones de proceso-a-proceso soportadas por los protocolos de Internet TCP/IP de la red informática

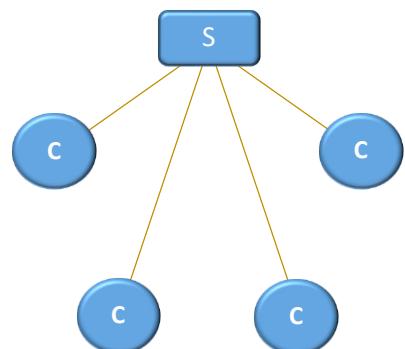
- El modelo TCP / IP no tiene capas de sesión o presentación porque no se consideraron necesarias.
 - En su lugar, las aplicaciones incluyen todas las funciones de sesión y presentación que requieren. Al final, la experiencia ha demostrado este punto de vista es el correcto
- La capa de aplicación gestiona el intercambio de datos entre procesos según dos modelos: cliente-servidor o peer-to-peer

La capa de aplicación

Modelo C/S vs. P2P



- Los protocolos de aplicación se diseñan conforme a dos modelos: Cliente/servidor (C/S) y de igual-a-igual (P2P)

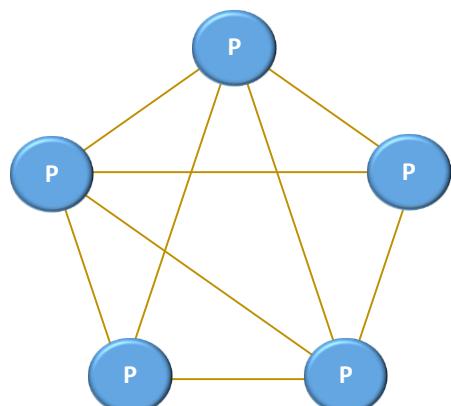


C/S

- El cliente es diferente del servidor
- Mayor velocidad de acceso
- La seguridad es mejor

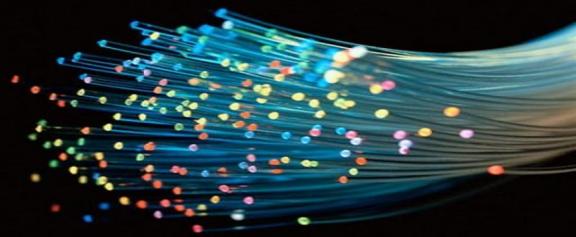
P2P

- Todos los nodos son iguales
- Menos seguras
- Aplicaciones en redes domésticas

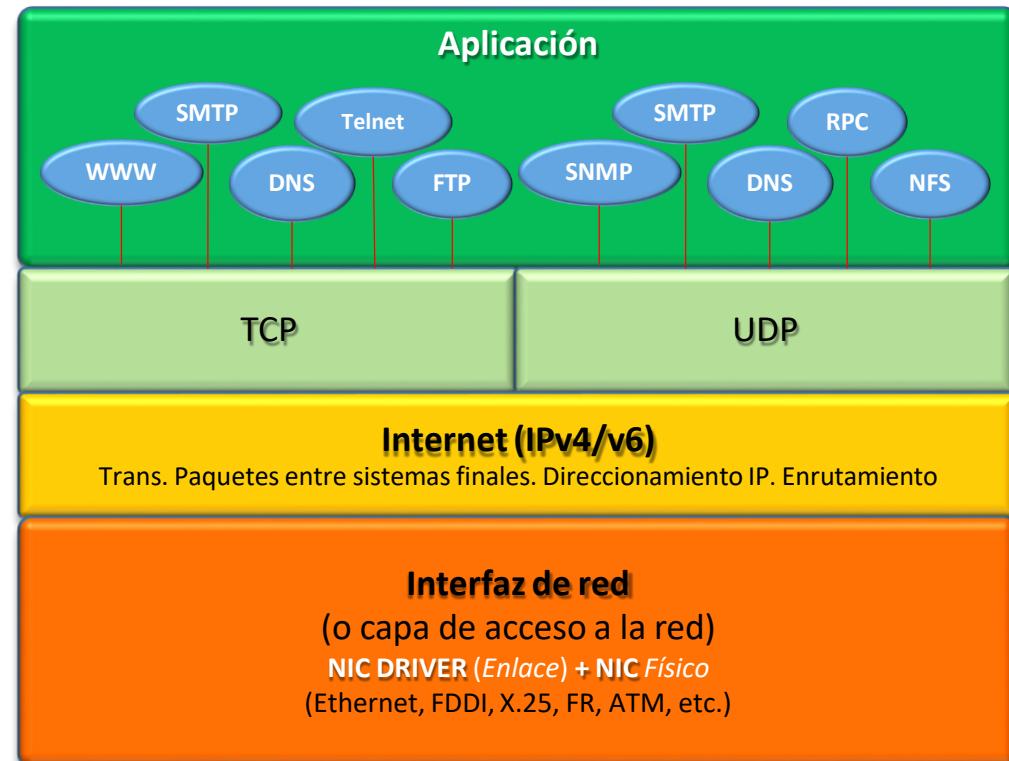


La capa de aplicación

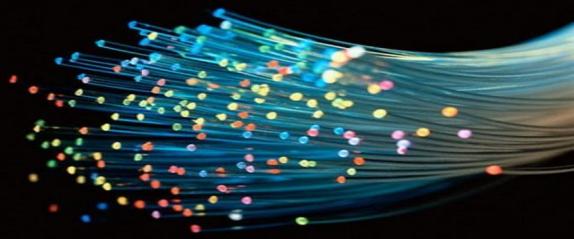
Protocolos especificados



- Muchos protocolos de la capa de aplicación de Internet están plenamente especificados el *Internet Engineering Task Force* en los RFCs y por lo tanto son del dominio público



El modelo C/S

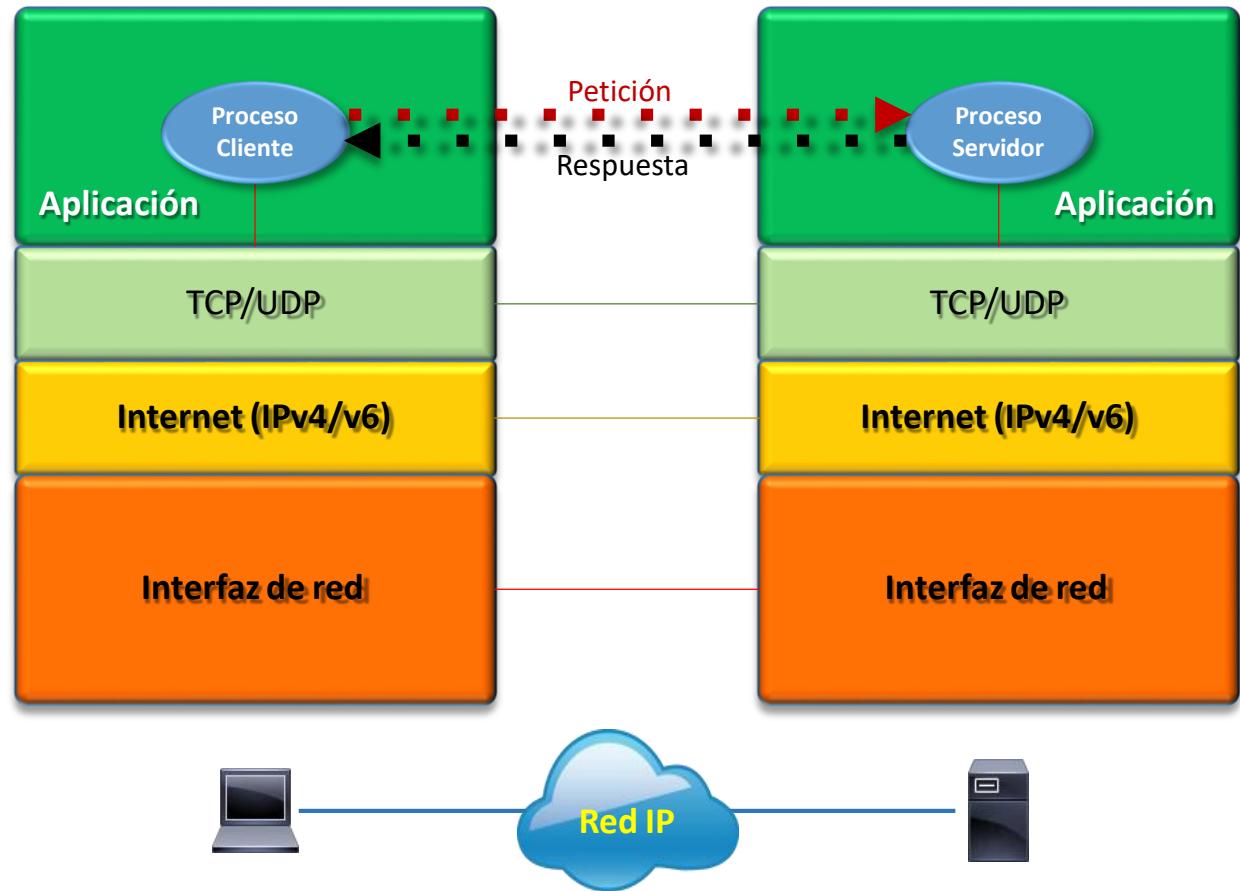


■ Servidor:

- Cualquier programa que ofrece un servicio que se puede obtener por la red
- Acepta peticiones, realiza el servicio y devuelve el resultado

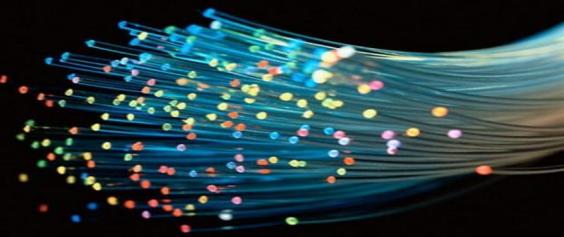
■ Cliente:

- Envía peticiones al servidor y espera una respuesta. Interactúa con el usuario



El protocolo de transferencia de archivos

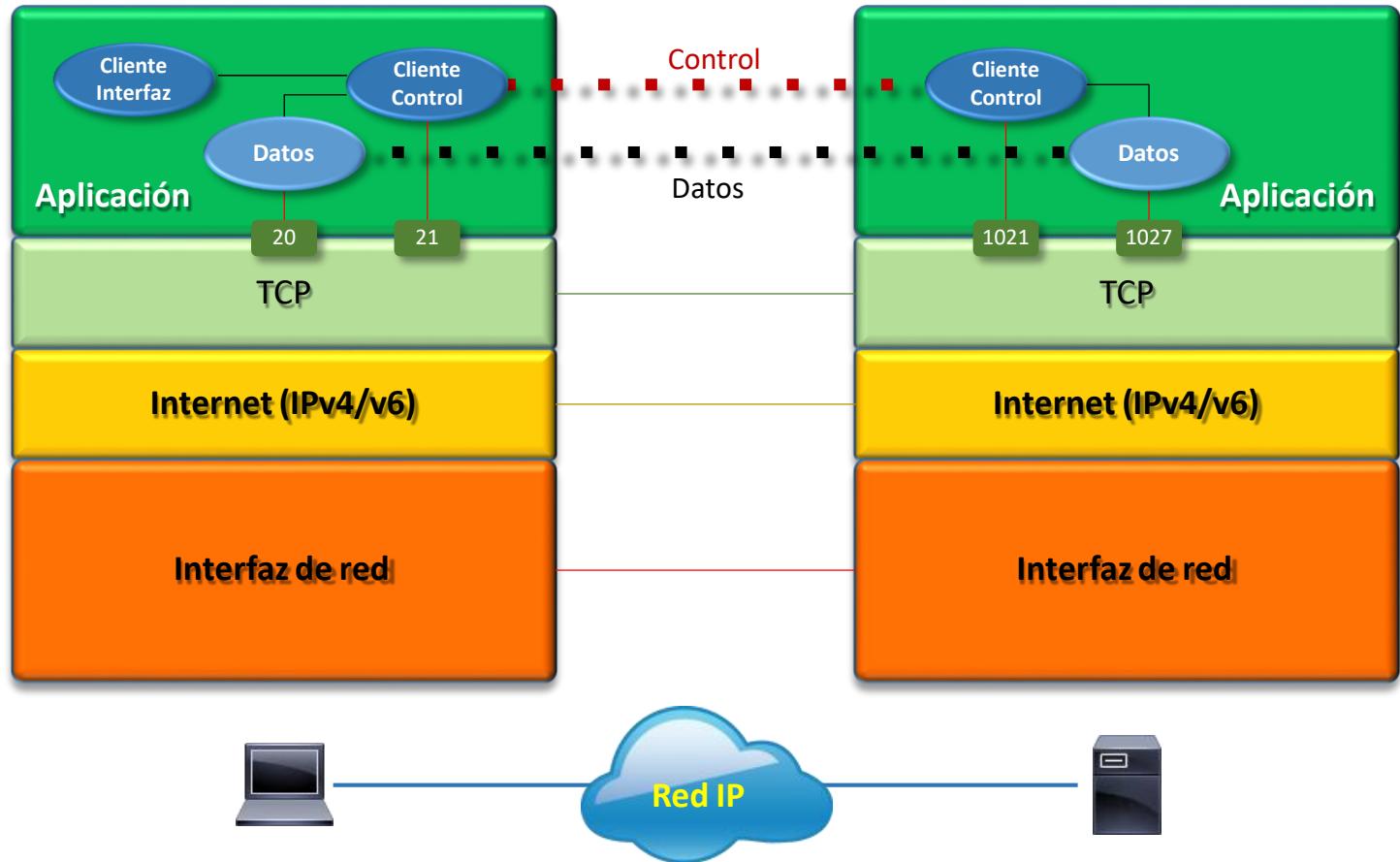
FTP (*File Transfer Protocol*)



- FTP es un protocolo para la transferencia de archivos entre sistemas conectados a una red TCP/IP basado en la arquitectura cliente-servidor

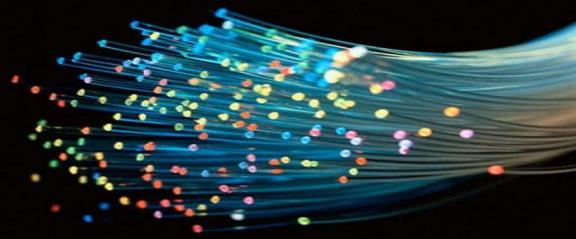
- Funcionamiento:

- En FTP se establecen dos conexiones TCP entre el cliente y el proceso servidor...
 - ✓ Conexión de Control. La inicia el cliente con el puerto 21 del servidor para el intercambio de mensajes de control.
 - ✓ Conexión de Datos: conexión bidireccional sobre la que se transfieren los datos en un modo y tipo especificados.



El sistema de nombres de dominio

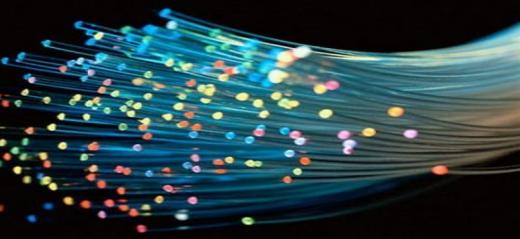
DNS (*Domain Name System*). Introducción



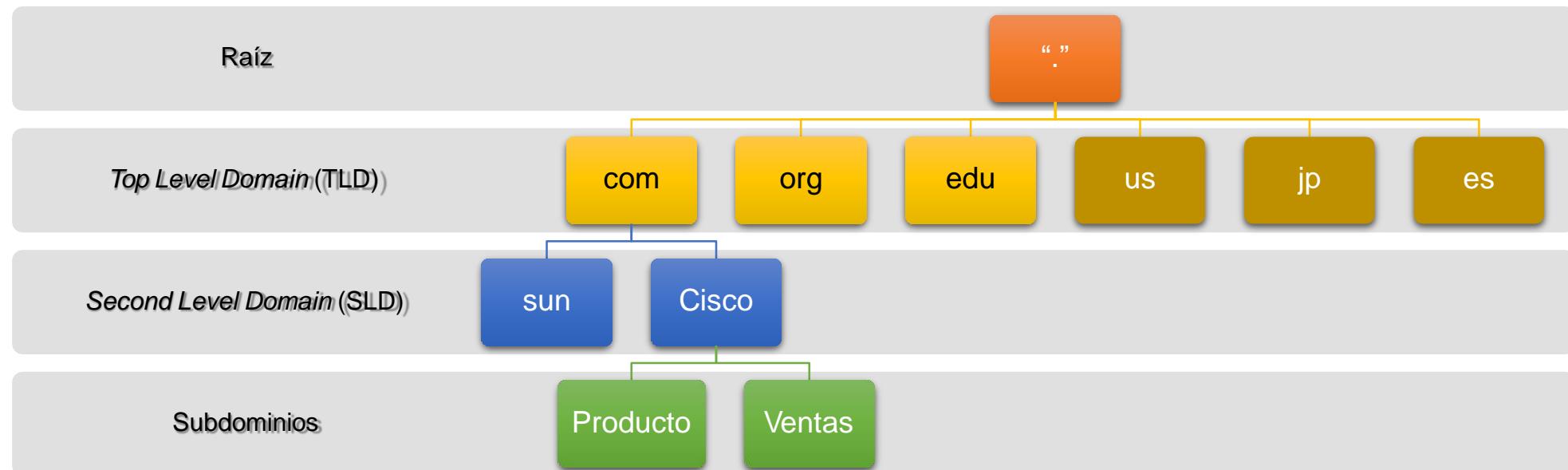
- La red Internet permite el acceso a una ingente cantidad de hosts y, en general, de recursos, la mayoría de los cuales se pueden referenciar mediante un nombre (de dominio) para que los usuarios de Internet no tengan que acceder a cada servicio utilizando la dirección IP
 - Por motivos de eficiencia y simplicidad todos los nombres de la red están organizados de una manera jerárquica, formando un sistema de dominios.
 - Para obtener información asociada a cualquier nombre, se utiliza un servicio que, funcionalmente, es como una base de datos distribuida:
 - ✓ se le hacen consultas, que pueden incluir una serie de criterios de selección, y responde con la información solicitada.

El sistema de nombres de dominio

Jerarquía DNS

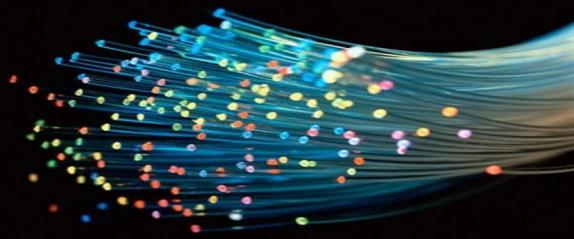


Un nombre de dominio puede estar formado por una o más cadenas de caracteres (etiquetas) separadas por puntos, y su estructura refleja la estructura jerárquica del Sistema de Nombres de Dominio (abajo indicado). La etiqueta que se encuentra más a la derecha se corresponde con el Dominio de Nivel Superior o TLD y así sucesivamente.

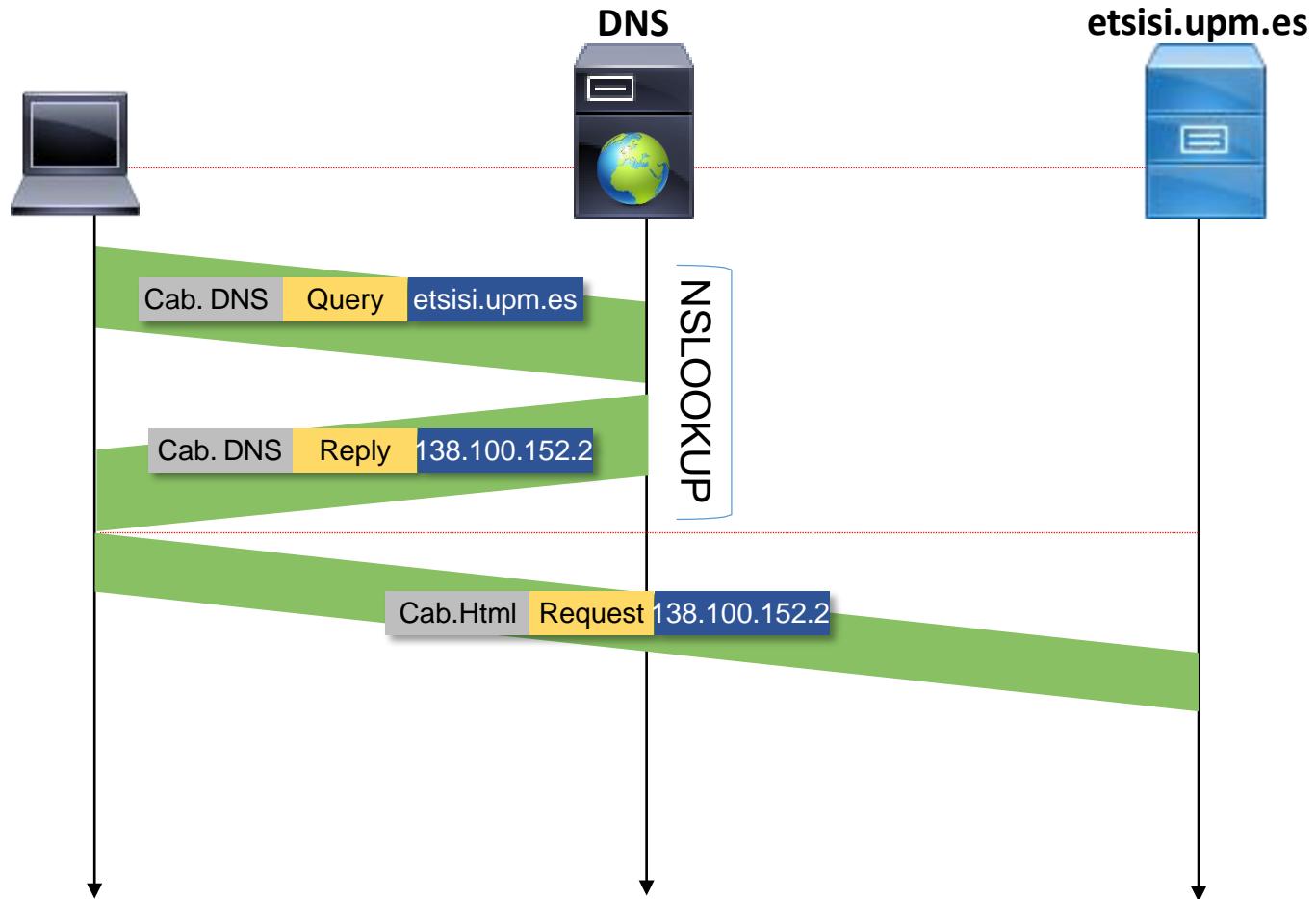


El protocolo DNS

Funcionamiento



- Las consultas son mensajes enviados a un servidor de nombres para obtener una respuesta. En Internet, las consultas se transportan en datagramas UDP.
 - La respuesta del servidor de nombres puede ser la respuesta en sí a la consulta, referencias a otro conjunto de servidores de nombres, o algún error.
 - Generalmente, el usuario no realiza las consultas directamente, las envía al resolver y éste envía una o más consultas a los servidores de nombres.



FIN

