
# Introducción a TCP/IP

# ¿Cómo funciona Internet?

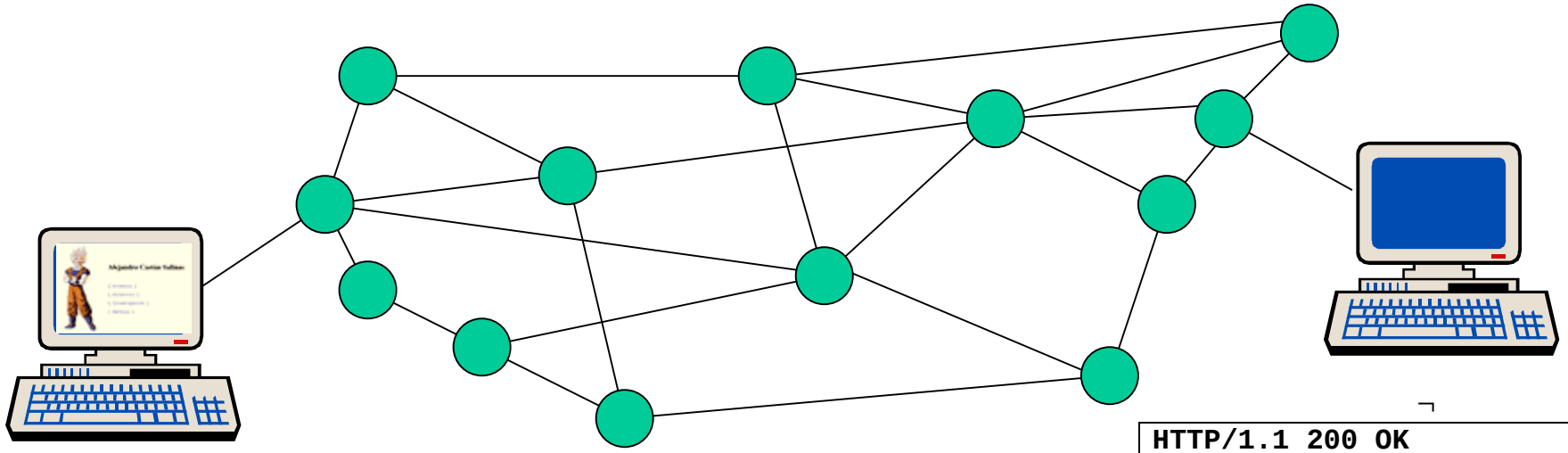
**Alejandro Castán Salinas**

acastan@xtec.net

# INTERNET (I)



**Dos ordenadores se comunican a través de Internet. La información puede atravesar decenas de nodos antes de llegar a su destino.**



®

```
GET /~acastan/index.html HTTP/1.1
Host: www.xtec.net
```

= Router

```
HTTP/1.1 200 OK
Date: Fri, 26 Sep 2003 12:38:06
Server: Apache/2.0.43 (Unix)
Accept-Ranges: bytes
Content-Length: 2227
Content-Type: text/html;
charset=ISO-8859-1

<html>
  <head>
    title>¡Hola!</title>
  </head>
  <body>
  ...
```

# INTERNET (II)



**Dos ordenadores se comunican a través de Internet. La información puede atravesar decenas de nodos antes de llegar a su destino.**

**La capacidad de enviar información de un extremo puede sobrepasar con creces la capacidad de recibir información del otro extremo, que puede ser más lento o estar saturado.**

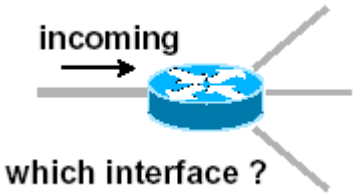
- **¿Cómo encuentra la información el camino desde el origen hasta el destino?**
- **¿Por qué llega la información sin errores?**
- **¿Por qué llega la información en el mismo orden que se envió?**
- **¿Por qué no se pierde parte de la información?**
- **¿Por qué no se mezcla la información, cuando un ordenador tiene al mismo tiempo abiertas dos aplicaciones que reciben datos de Internet?**

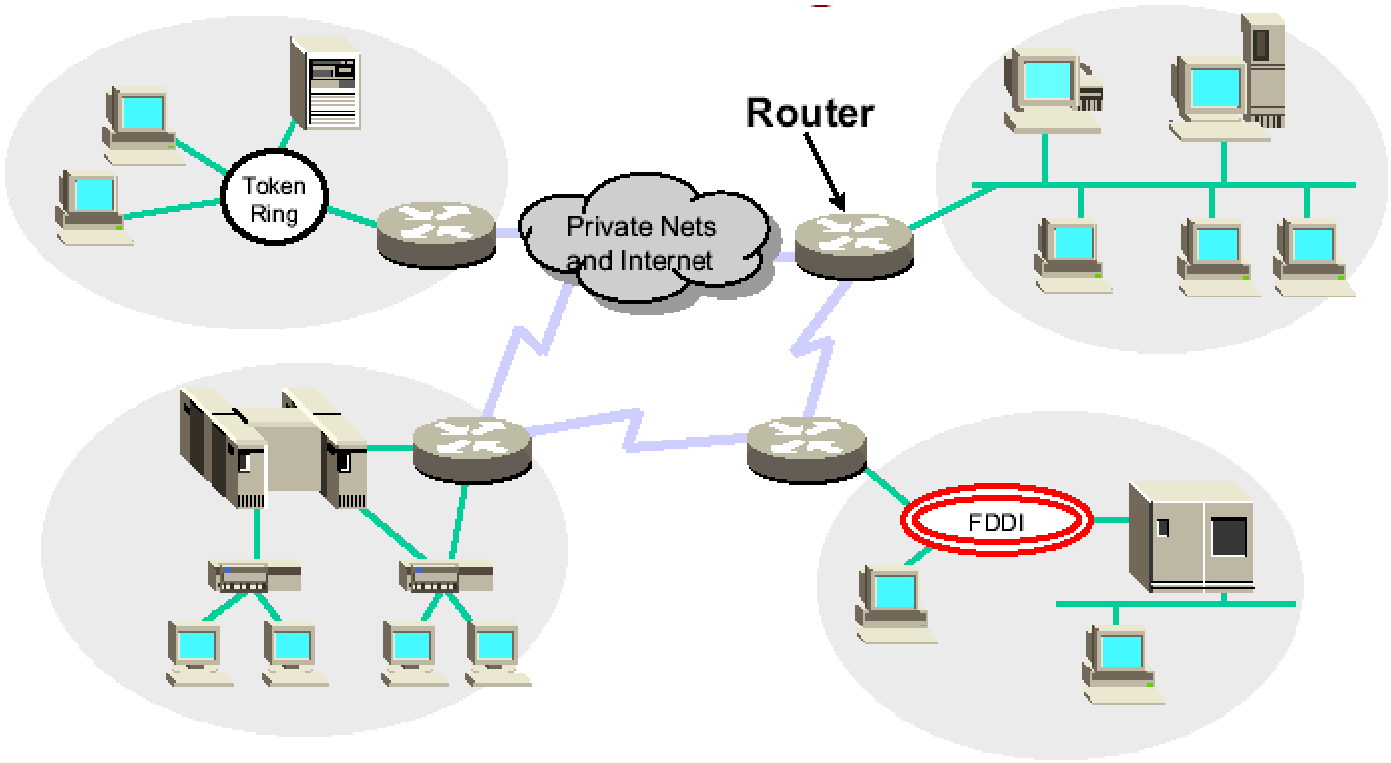
# INTERNET (III)



- **Conecta ordenadores, independientemente del sistema operativo, formando redes.**
- **Conecta redes, independientemente de sus diferentes topologías y del hardware de red, formando redes más amplias.**
- **TCP/IP es la familia de protocolos (IP, TCP, UDP, ICMP, ...) encargados de la transmisión de los paquetes de información.**
- **Es una especificación abierta y no propietaria.**
- **IETF: desarrolla estándares y protocolos.**
  **NIC: asigna nombres de dominio y direcciones únicas.**
  **IANA: asigna nombres de servicios.**

- **El encaminamiento de paquetes fuera de la red local lo realiza un router, buscando en la tabla de encaminamiento y decidiendo por cual interfaz de red enviarlos.**



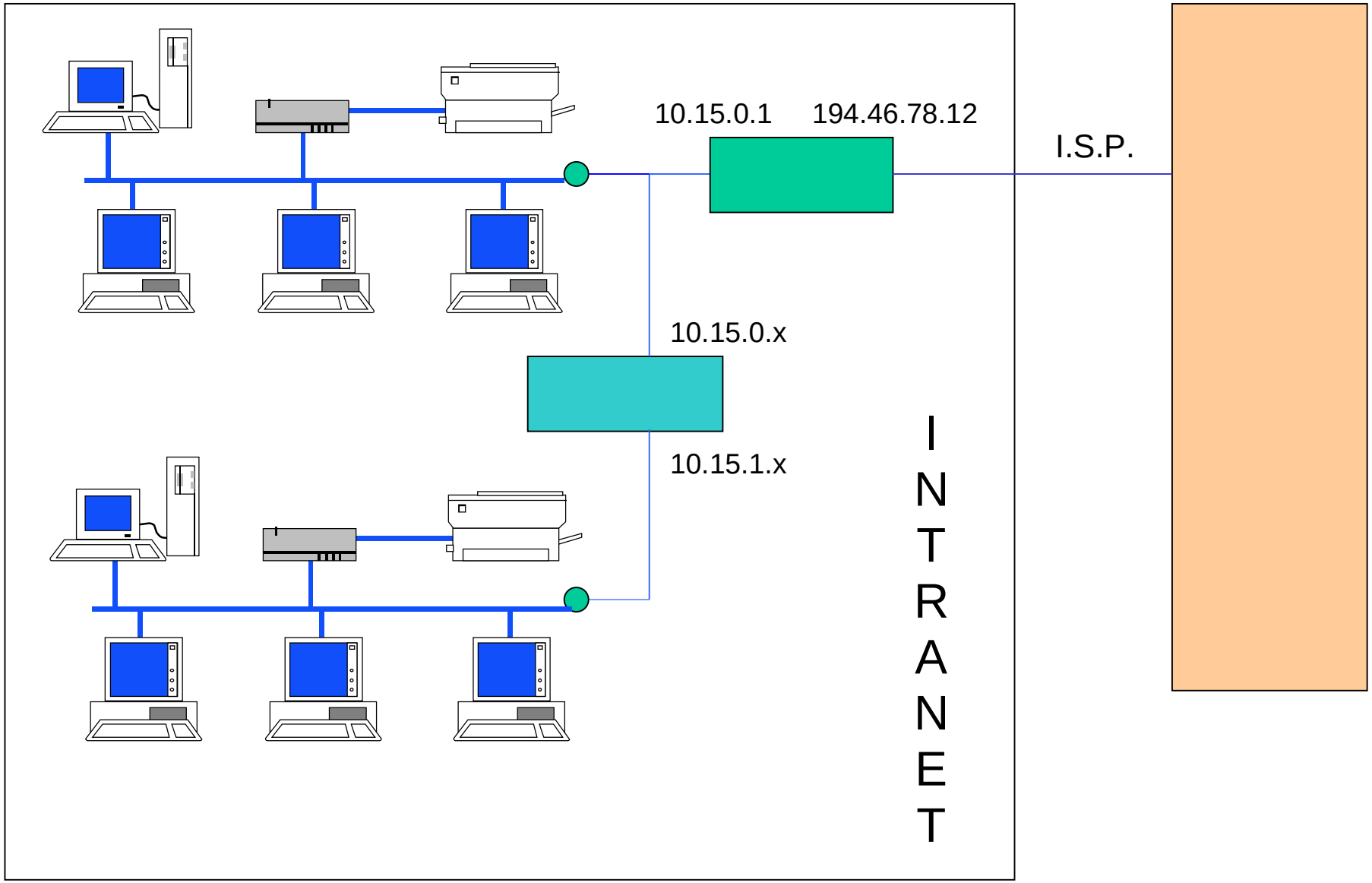
# INTRANET (I)



- **Es una Internet corporativa, aislada de Internet.**
- **Aprovecha la tecnología de Internet (aplicaciones, protocolos, ...) para una red corporativa.**
- **Utiliza direcciones IP privadas.**
- **Se puede conectar a Internet mediante algún dispositivo de red que transforme las direcciones IP privadas en públicas:**
  - **Un router con NAT (Network Adress Translation) o PAT (Port Adress Translation).**
  - **Un ordenador que realize IP masquerading, que además puede incormorar un cortafuegos y un proxy-cache.**

# INTRANET (II)





# HISTORIA DE INTERNET[1] Y TCP/IP[2]

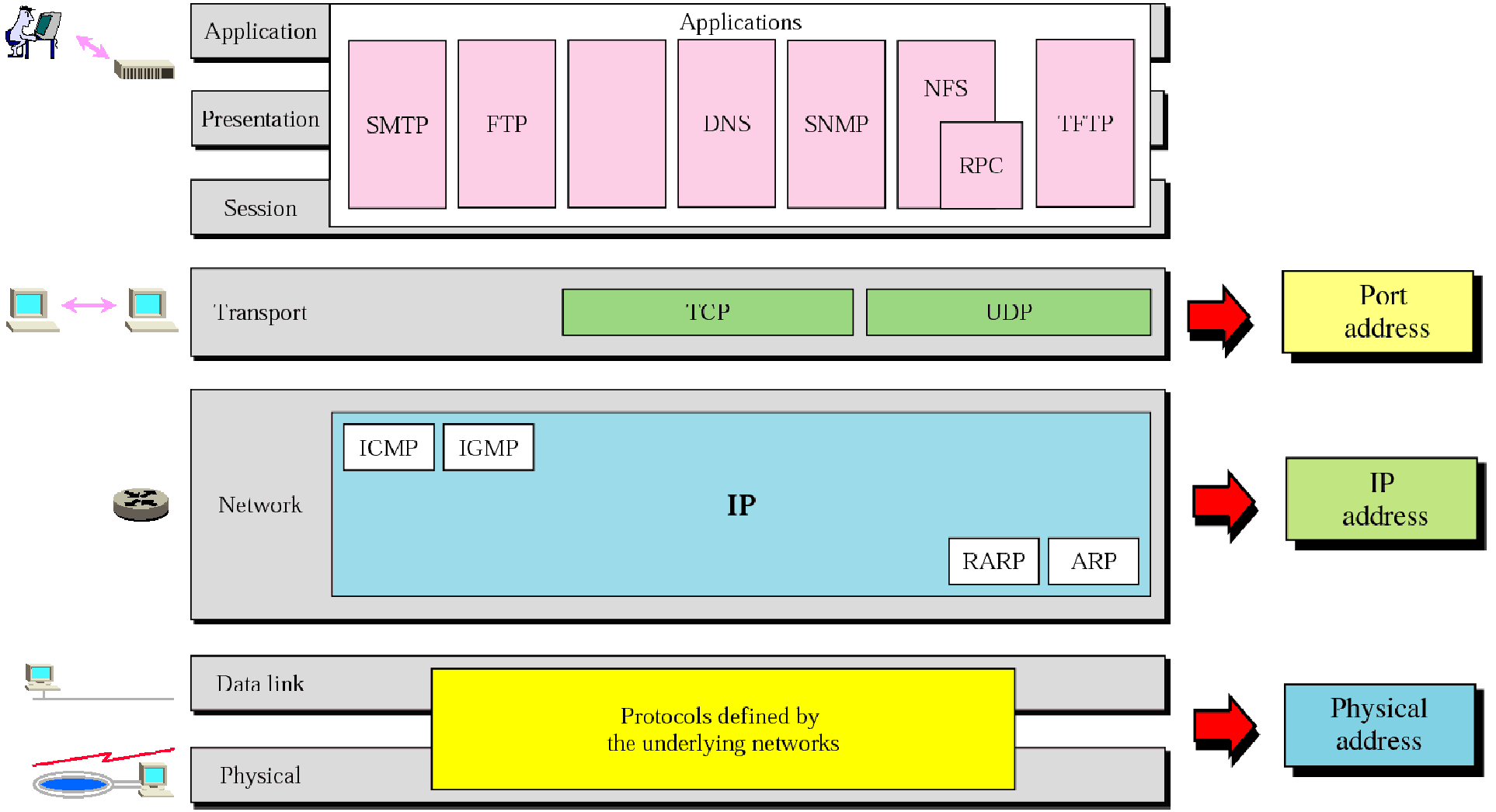


- **1957 USSR Sputnik, USA funda ARPA**
- **1969 ARPA funda ARPANET**
- **1971 Red con 15 nodos**
- **1974 Protocolo Cerf/Kahn**
- **1973 Ethernet**
- **1982/83 TCP/IP protocolo central**
- **1983 4.2BSD - primera implementación TCP/IP disponible**
- **1986 4.3BSD - mejoras de rendimiento**
- **1988 4.3BSD Tahoe - añade inicio lento, control de congestión y retransmisión rápida.**
- **1990 4.3BSD Reno - añade predicción de cabecera TCP, compresión SLIP y una nueva tabla de encaminamiento.**
- **1993 4.4BSD - añade multicasting.**

[1] Historia de Internet: http://www.isoc.org/internet/history/
[2] Historia de TCP/IP: http://www.cs.utexas.edu/users/chris/think/Early_Days_Of_TCP/index.shtml

# NIVELES Y PROTOCOLOS(I)





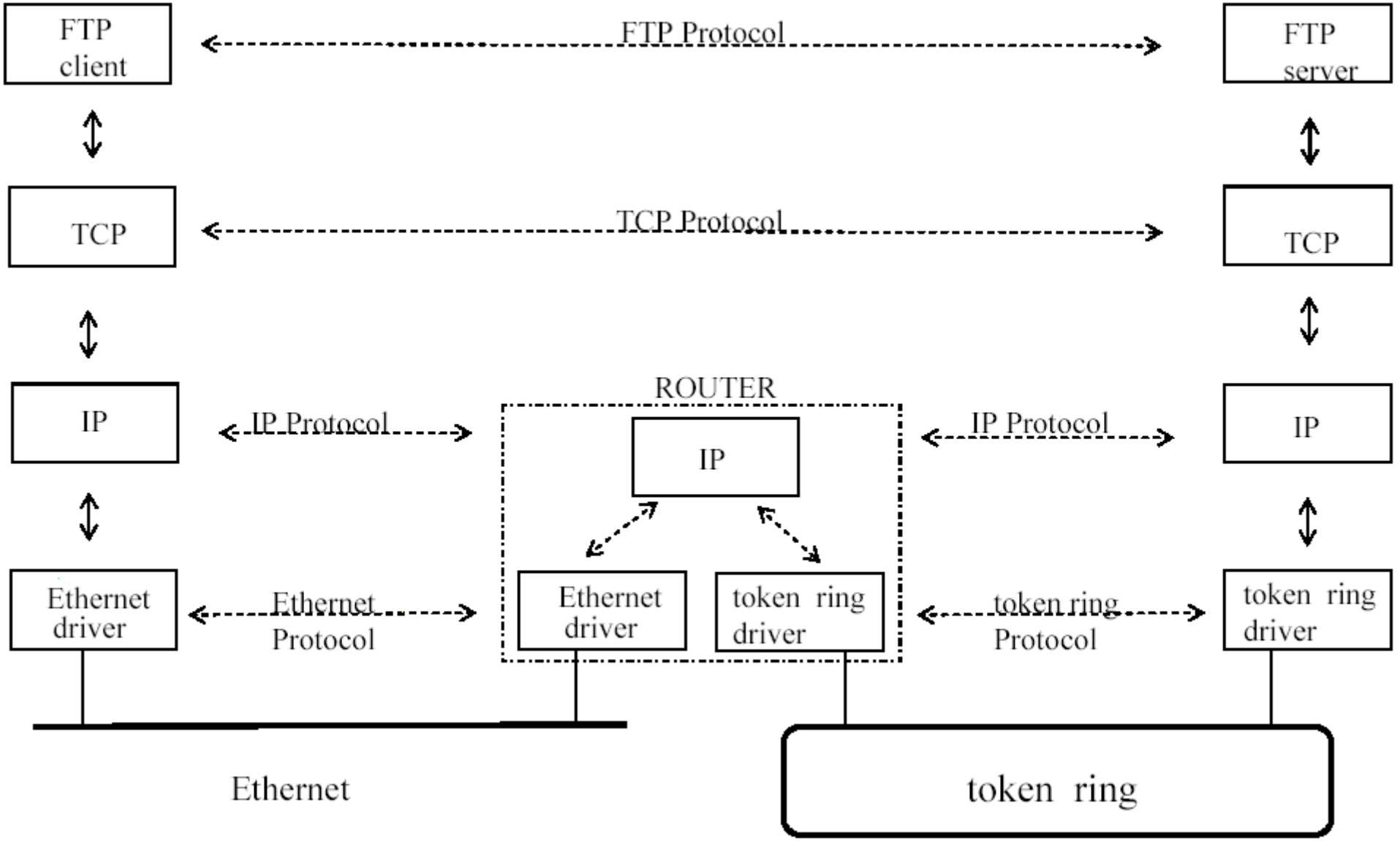
# NIVELES Y PROTOCOLOS (II)



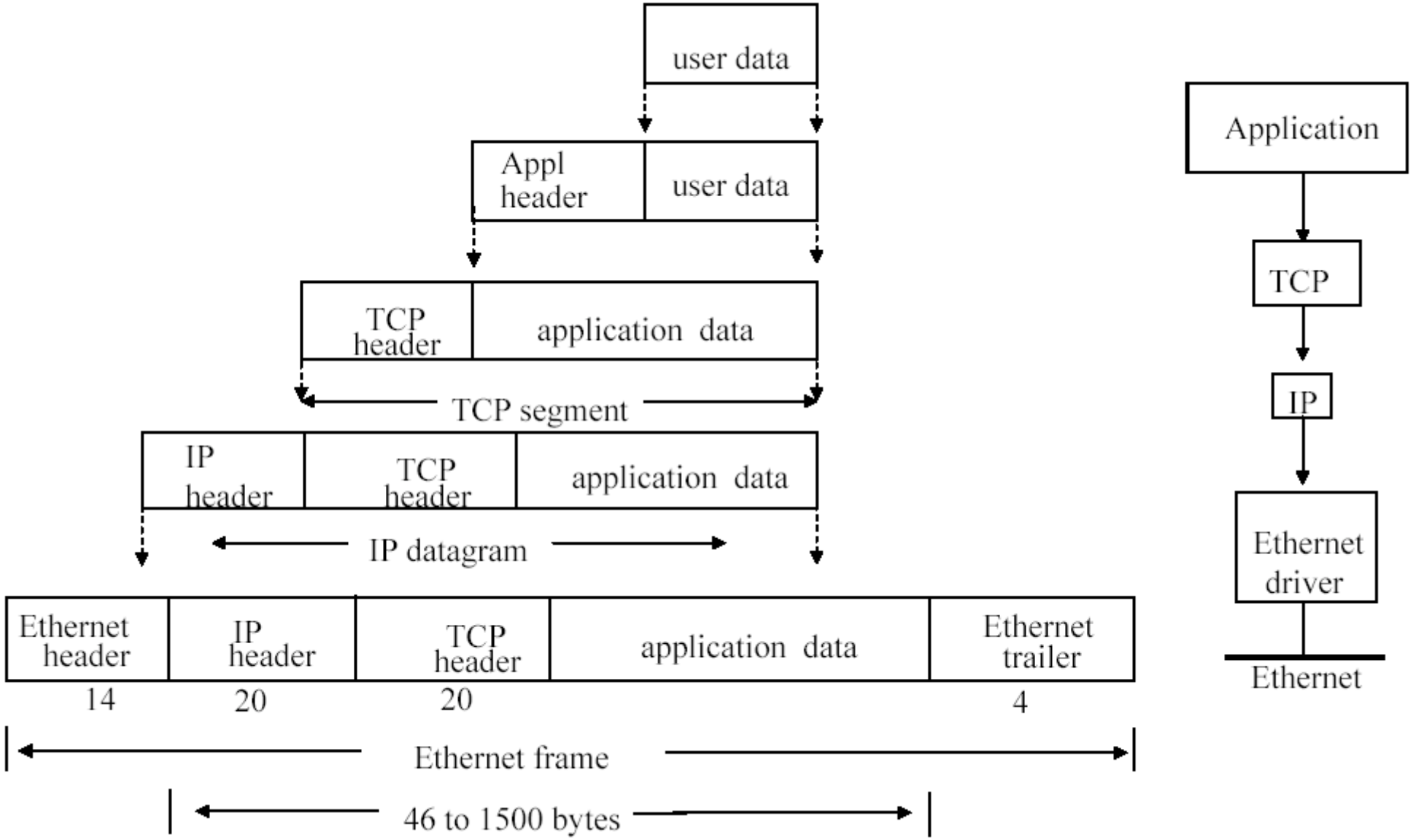
- **IP: encargado de que los datos lleguen a su destino, escogiendo el camino por el que enviar los paquetes de información.**
- **TCP: encargado de que la información se reconstruya de forma correcta cuando llegue a su destino, para pasarla a la aplicación.**
- **UDP: lo mismo que TCP pero en sencillo (más inseguro pero más rápido).**
- **ICMP: mensajes de error que ayudan al nivel IP.**
- **DNS: convierte nombre de Internet (nombre_máquina.nombre_dominio) en dirección de Internet (IP).**
- **ARP: convierte dirección de Internet (IP) en dirección física (MAC).**

# NIVELES Y PROTOCOLOS (III)



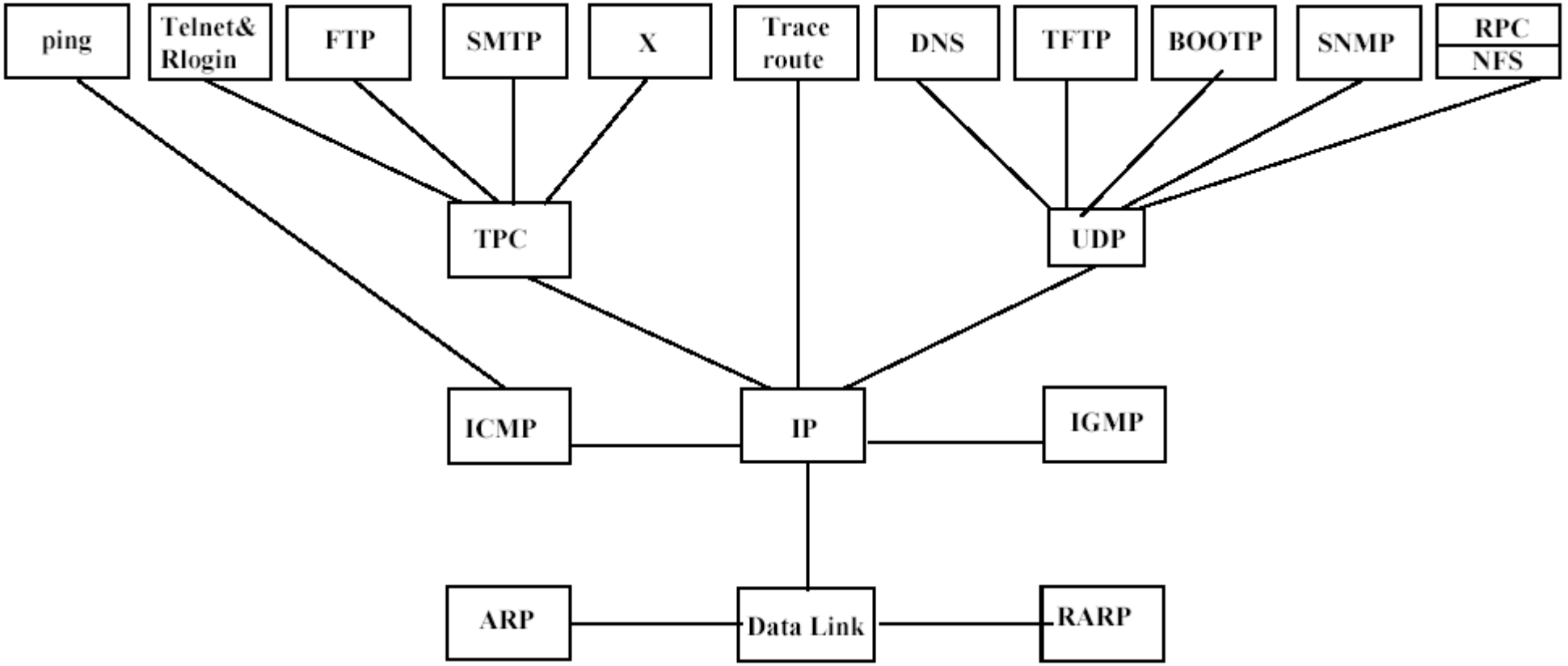


# NIVELES Y PROTOCOLOS (IV)



# NIVELES Y PROTOCOLOS (V)

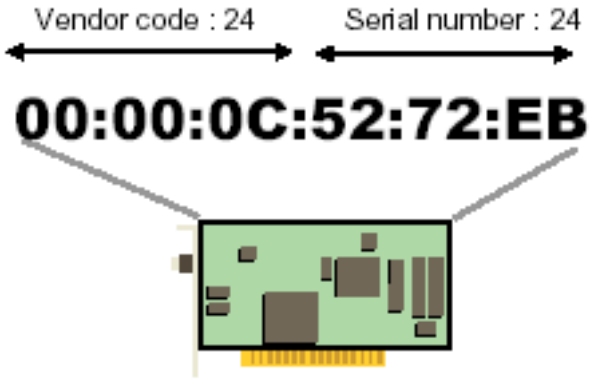




# DIRECCIONES FÍSICAS

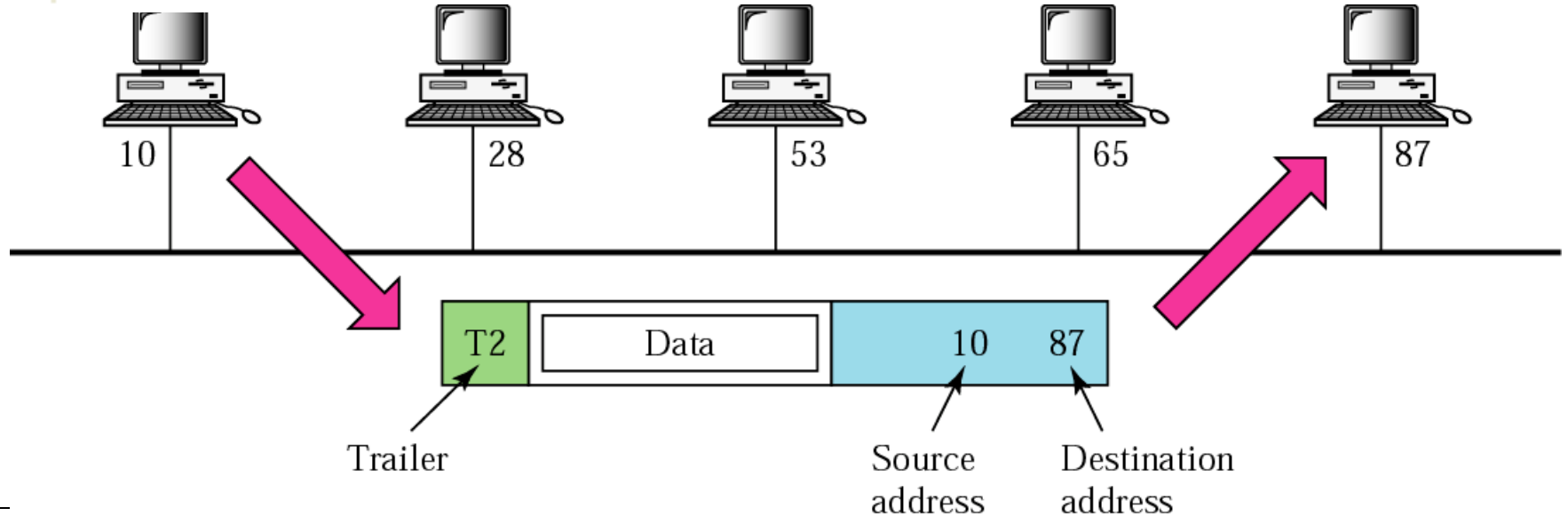


**Normalmente, en redes locales se usa una dirección física de 48 bits (6 bytes), escrita como 12 dígitos hexadecimales separados dos a dos por un guión. Es la dirección hardware (MAC) asignada a la tarjeta de red.**




**La dirección MAC está "grabada" en hardware dentro de la tarjeta de red[3].**

**En UNIX se puede consultar la dirección de red con los comandos `ifconfig -a` y `netstat -ie`.**




[3] Se pueden consultar los datos del vendedor de la tarjeta de red, en http://standards.ieee.org/cgi-bin/ouisearch?xx-xx-xx (donde xx-xx-xx son 6 primeros dígitos hex MAC)

# DIRECCIONES IP (I)



**En IPv4, la dirección IP tiene una longitud de 32 bits, expresada como cuatro números decimales de un byte separados por un punto.**

Por ejemplo: 132.24.75.9

**Una máquina puede tener más de una dirección IP, cada una asociada a su interfaz de red. En UNIX se puede consultar la dirección IP con los comandos** `ifconfig -a` **y** `netstat -ie`**.**

- **Públicas: Son asignadas por el N.I.C. (se paga por su utilización) y hacen que el ordenador sea "visible" en Internet.**

- **Privadas: me las asigno yo mismo y el ordenador no es "visible" en Internet.**

10.0.0.0 $\rightarrow$ 10.255.255.255
172.16.0.0 $\rightarrow$ 172.31.255.255
192.168.0.0 $\rightarrow$ 192.168.255.255

- **Loopback: usadas para comunicarse una aplicación cliente con una aplicación servidor en la misma máquina:** 127.x.x.x

# DIRECCIONES IP (II)

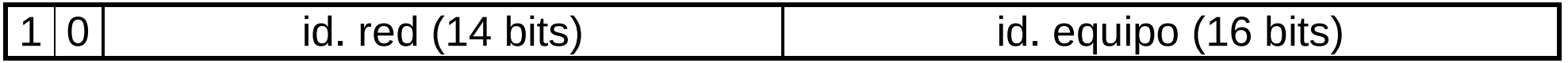


- **El identificador de equipo “todo ceros” está reservado para especificar el número de red. Por ejemplo:** 192.150.30.0

- **El identificador de equipo “todo unos” está reservado para especificar la dirección de broadcast de la red. Por ejemplo:** 192.150.30.255

Clase A: 0.0.0.0 a 127.255.255.255 $2^{24}$ - 2 = 16.777.214 direcciones usables


Clase B: 128.0.0.0 a 191.255.255.255 $2^{16}$ - 2 = 65.534 direcciones usables




Clase C: 192.0.0.0 a 223.255.255.255 $2^{8}$ - 2 = 254 direcciones usables


Clase D: 224.0.0.0 a 239.255.255.255


Clase E: 240.0.0.0 a 255.255.255.255

# DIRECCIONES IP (III)



- **Las subredes se asignan dividiendo el identificador de equipo en dos piezas de longitud apropiada: la dirección de subred más la dirección de equipo.**

| | ← id. equipo → | |
|---|---|---|
| id. red | dir. subred | dir. equipo |

**Por ejemplo, la dirección de clase B** 158.108 **puede utilizar su tercer byte para identificar la subred:** 158.108.1.X **,** 158.108.2.X **, ... donde X es una dirección de equipo que va de 1 a 254.**

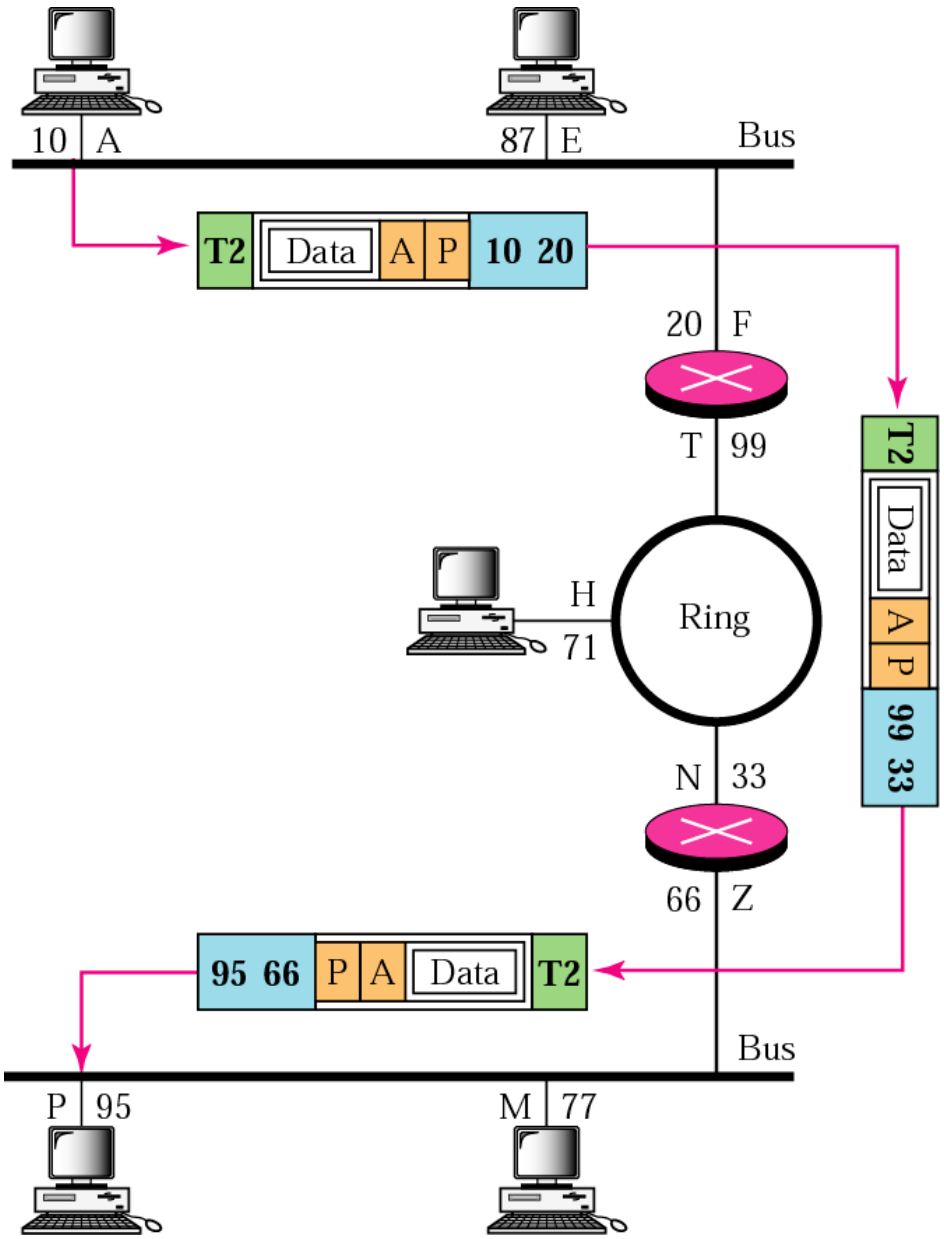
- **La máscara de subred es un número de 32 bits que indica al router cómo reconocer el campo de subred. Este número se crea cubriendo con bits 1 la dirección de red y subred, y con bits 0 la dirección de equipo.**

| | | |
|---|---|---|
| 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 | 1 1 1 1 1 1 1 1 | 0 0 0 0 0 0 0 0 |

**En el ejemplo anterior, la máscara de subred seria** 255.255.255.0

# DIRECCIONES IP (IV)



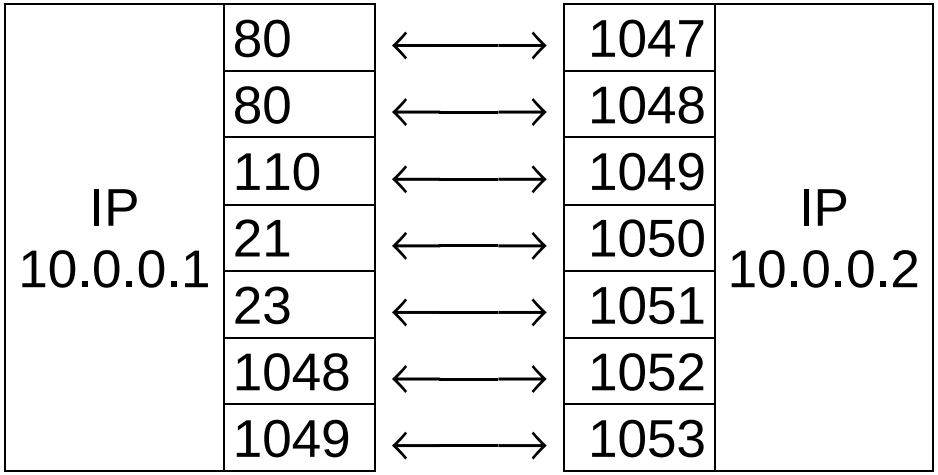


# DIRECCIONES DE PUERTOS (I)



**Un usuario puede a la vez utilizar varias aplicaciones que trabajen a través de Internet. Por ejemplo puede:**
**- Estar consultando una o más páginas Web (protocolo HTTP)**
**- Estar recuperando su correo electrónico (protocolo POP3)**
**- Estar bajando un fichero (protocolo FTP)**
**- Estar conectado a otro ordenador (protocolo TELNET)**

**Recibirá una serie de paquetes con información de distinto tipo que es necesario distinguir a qué aplicación pertenecen. La dirección IP solo vale para saber que van dirigidos a nuestro ordenador. Necesitamos información extra en el paquete para identificar el tipo de información que contiene.**




←Petición

| Origen | Destino | |
|---|---|---|
| 10.0.0.2:1047 | 10.0.0.1:80 | mensaje |

Respuesta →

| Origen | Destino | |
|---|---|---|
| 10.0.0.1:80 | 10.0.0.2:1047 | mensaje |

# DIRECCIONES DE PUERTOS (II)

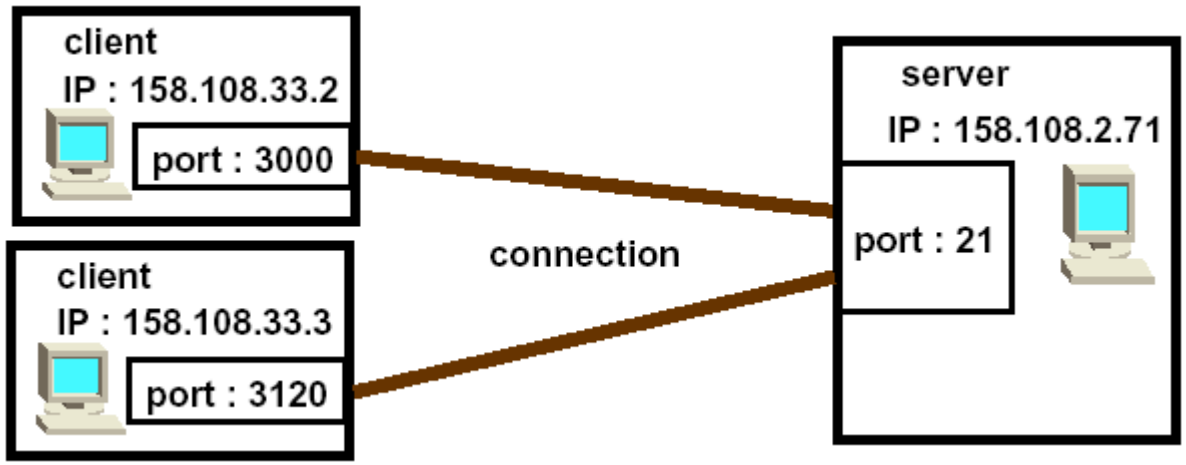


**La dirección de un puerto es un número de 16 bits, expresado como un número decimal.**

- **Los números de puertos están divididos en tres rangos:**
  **- puertos bien conocidos (del 0 al 1023),**
  **- puertos registrados (del 1024 al 49151) y**
  **- puertos dinámicos y/o privados (del 49152 hasta el 65535).**

- **En UNIX se puede consultar el estado de los puertos abiertos con el comando** `netstat -apen`**, y ver la lista de puertos bien conocidos consultando el fichero** `/etc/services`**.**

- **Un mismo puerto de un servidor puede ser accedido simultáneamente por varios clientes.**



# DIRECCIONES DE PUERTOS (III)

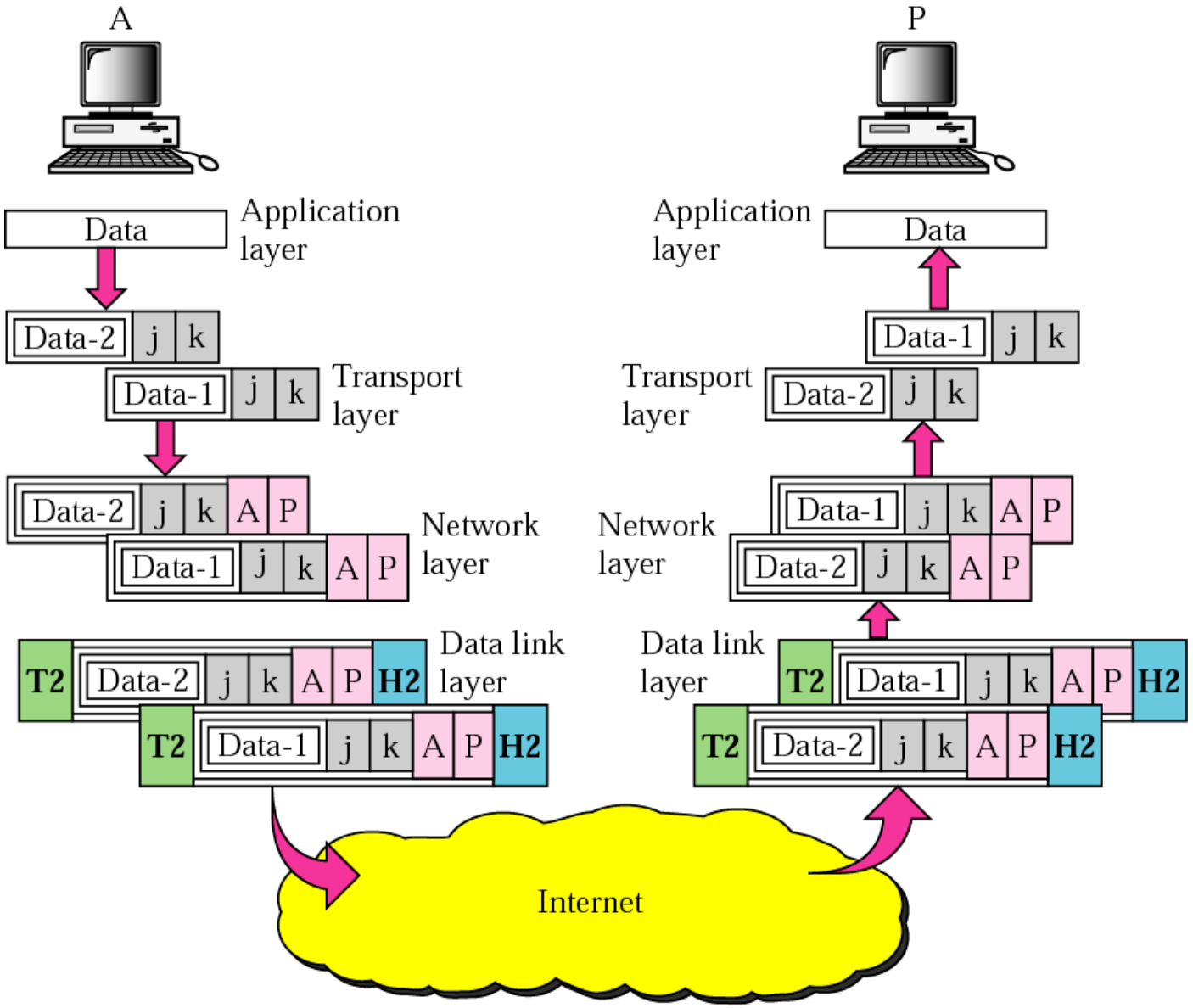


**Ejemplos de puertos bien conocidos con sus protocolos/aplicaciones asoc.:**

| | | | |
|---|---|---|---|
| **FTP** | **21** | **tcp** | **Protocolo de transferencia de ficheros** |
| **SSH** | **22** | **tcp** | **Conexión de terminal segura** |
| **TELNET** | **23** | **tcp** | **Conexión de terminal** |
| **HTTP** | **80 y 80xx** | **tcp** | **World Wide Web** |
| **HTTPS** | **443** | **tcp** | **World Wide Web segura** |
| **SMTP** | **25** | **tcp** | **Protocolo de transporte de correo** |
| **POP3** | **110** | **tcp** | **Transferencia de correo** |
| **IMAP** | **143** | **tcp** | **Consulta de correo** |
| **DNS** | **53** | **udp/tcp** | **Servidor de nombres de dominios** |
| **DHCP server** | **67** | **tcp/udp** | **Servidor de configuración de IP** |
| **DHCP client** | **68** | **tcp/udp** | **Cliente de configuración de IP** |
| **PORTMAP/RPCBIND** | **111** | **tcp/udp** | **Llamada a procedimiento remoto** |
| **LDAP** | **389** | **tcp/udp** | **Protocolo de acceso** |
| **NFS** | **2049** | **tcp/udp** | **Compartición de ficheros en Unix** |
| **NetBIOS/SAMBA** | **137-139** | **tcp** | **Compartición de ficheros en Windows** |
| **X11** | **6000-6255** | **tcp** | **Servidor X Windows** |

# DIRECCIONES DE PUERTOS (IV)





# TRANSFORMAR DIRECCIONES



**nontri.ku.ac.th**

⇓ DNS

**158.108.2.71**

⇓ ARP

**00:00:0C:06:13:4A**

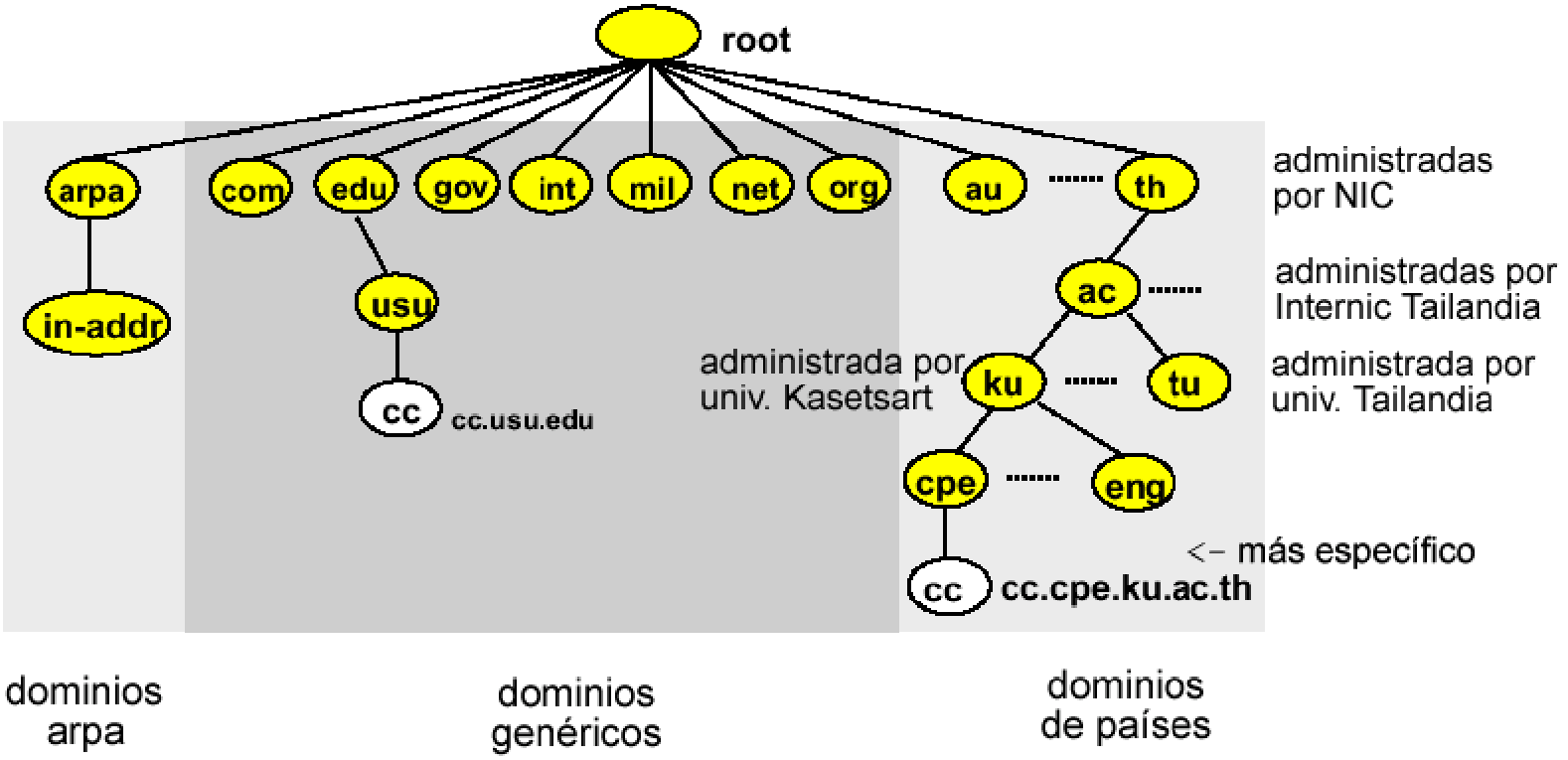
- **Transformar el nombre en dirección IP:**
  **- En la red local: tabla ‘hosts’ o servidor DNS.**
  **- En Internet: servidores DNS.**

- **Transformar la dirección IP en dirección de red**
  **- En la red local: ARP**
  **- En Internet: dirección de red del router.**

# DNS[4]

- **El servidor DNS (puerto 53) guarda la relación de los nombres e IPs en un dominio. Utiliza una cache para reducir el tráfico DNS.**

- **Utiliza protocolo UDP para la petición y respuesta, pero si la respuesta es muy grande usa el protocolo TCP para devolverla.**

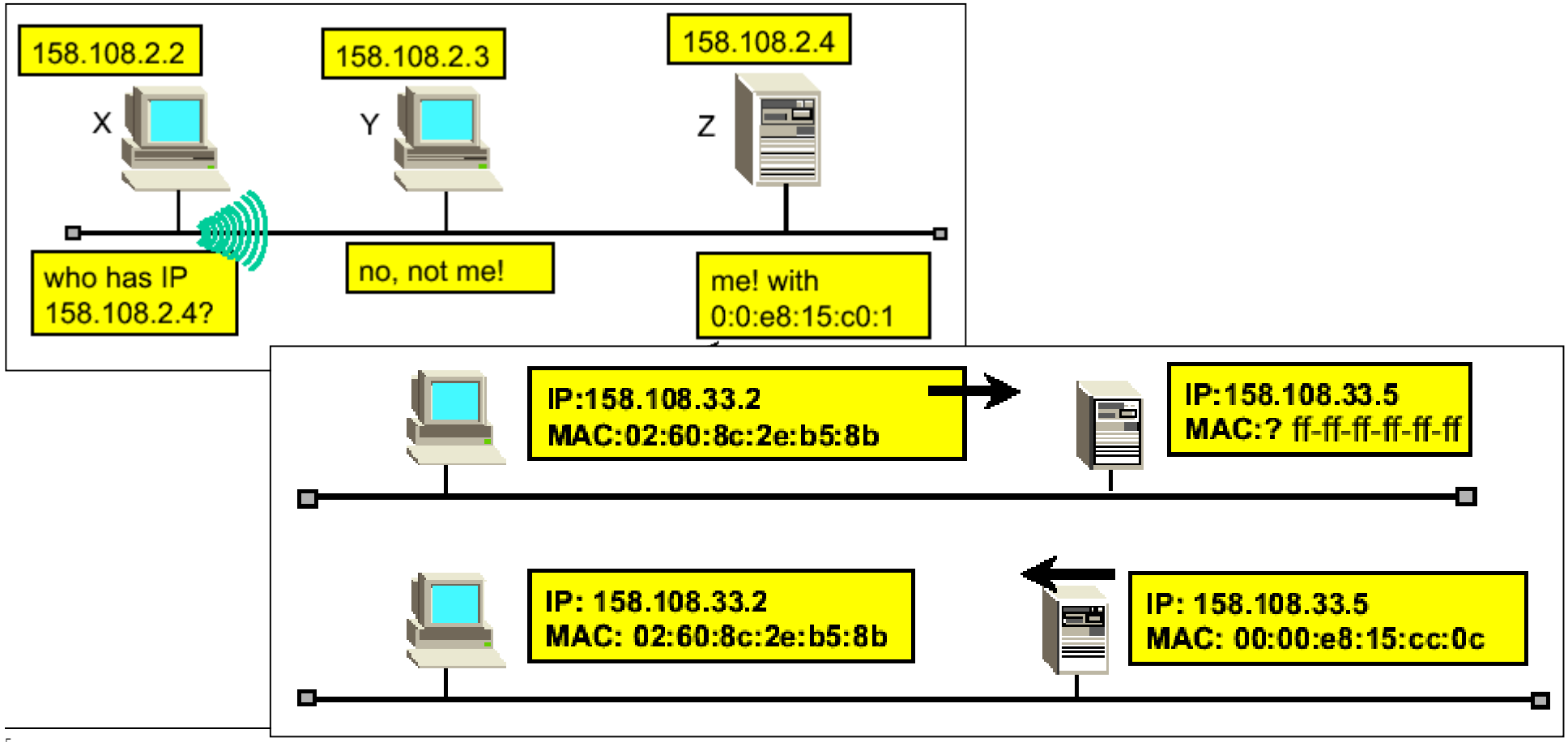



[4] http://www.faqs.org/rfcs/rfc1591.html o ftp://ftp.rfc-editor.org/in-notes/rfc1591.txt - Servidores DNS raíz: http://www.root-servers.org/

# ARP[5]

**Cuando un equipo de una red quiere obtener la dirección MAC de otro:**

1. **Envía una solicitud ARP a la dirección MAC de broadcast (**ff-ff-ff-ff-ff-ff**).**
2. **Recibe una respuesta ARP del equipo, con su MAC (la guardará en tabla).**

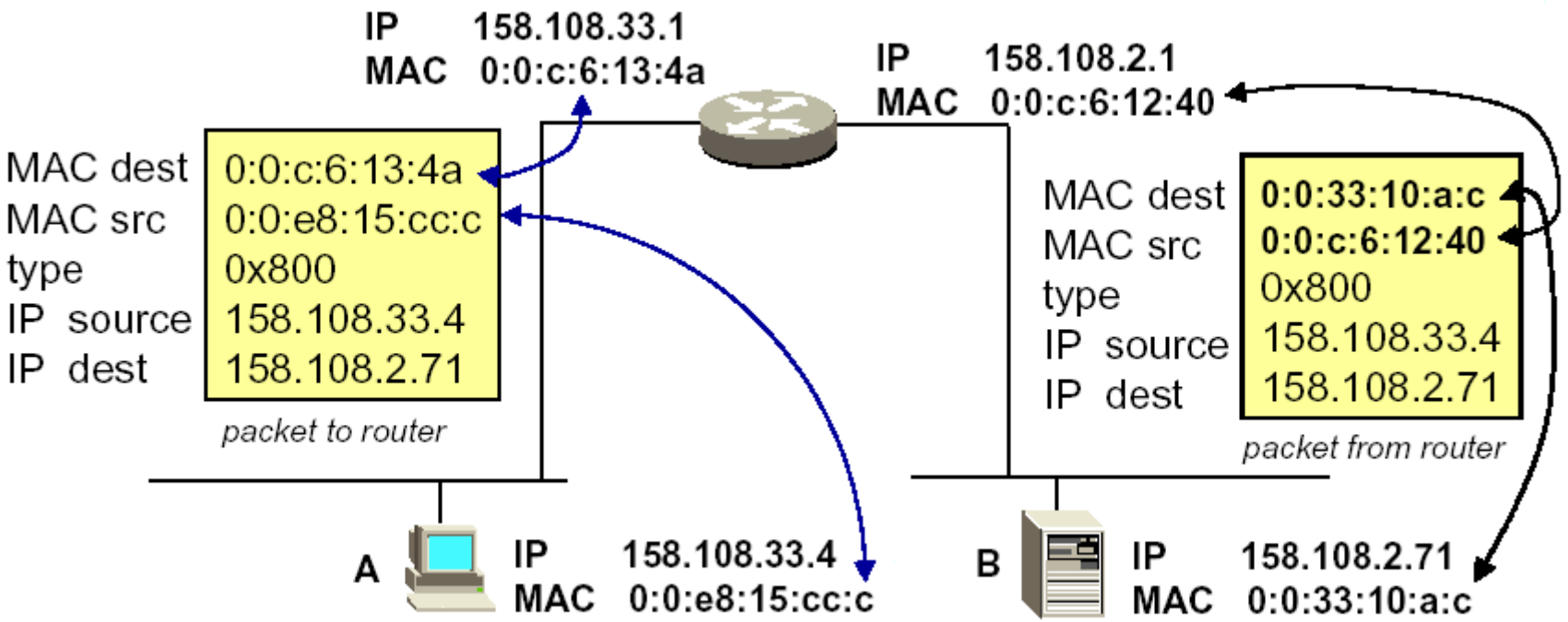



[5] http://www.faqs.org/rfcs/rfc826.html o ftp://ftp.rfc-editor.org/in-notes/rfc826.txt

- **Un router contiene una tabla de encaminamiento que indica que conexión debe usarse para alcanzar cada red, y una indicación del rendimiento de dicha conexión.**

- **Se puede consultar dicha tabla con el comando Unix** `netstat -rn`

- **Se pueden añadir manualmente entradas a dicha tabla con el comando Unix** `route add <IP> <gateway>`



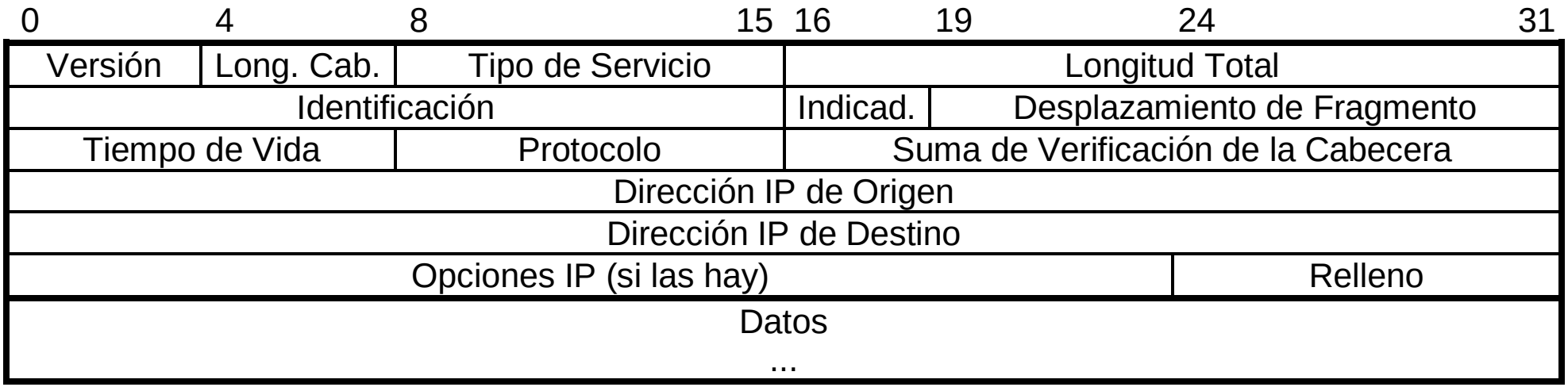
# IP (I)[6]



**IP es el protocolo encargado de que los datos lleguen a su destino, escogiendo el camino por el que enviar los paquetes de información (datagramas).**

- **Los paquetes pueden perderse, llegar duplicados y/o en secuencia diferente a como se enviaron.**

| cabecera ethernet | cabecera IP | datos (paquetes TCP, UDP, ICMP, IPv6, ARP, ...) |
|---|---|---|




[6] http://www.faqs.org/rfcs/rfc791.html o ftp://ftp.rfc-editor.org/in-notes/rfc791.txt

# IP (II)

- **Versión (del protocolo IP): formato de la cabecera (IPv4 = 4, IPv6 = 6).**
- **Long. cab.: longitud de la cabecera IP en múltiplo de 32 bits (sin opciones = 5, con opciones = ?).**
- **Tipo de servicio (TOS): Se utiliza para la priorización de paquetes IP.**
  **- Bits 0-2 (precedencia): nivel de prioridad del paquete.**
  **- Bits 3-6 (tipo de servicio): cómo debe la red equilibrar entre espera, rendimiento, fiabilidad y coste al encaminar el paquete IP.**
  **- Bit 8 (MBZ): no se utiliza y debe ser cero.**
- **Longitud total: longitud en bytes del paquete IP (incluyendo la cabecera).**
- **Número de identificación, indicadores y desplazamiento de fragmento: se utilizan para el seguimiento de las partes cuando un paquete se deba partir, por ejemplo, porque se reenvíe por una red para la cual es demasiado grande.**
- **Tiempo de vida: Número máximo de routers a través de los que puede pasar el paquete IP. Dicho número se decrementa cada vez que el**

**paquete pasa a través de un sistema. Cuando llega a cero, el paquete se destruye y se envía un mensaje ICMP al origen.**

- **Protocolo: número que indica cual es el protocolo del paquete contenido dentro de la sección de datos del paquete IP (1 = ICMP, 6 = TCP, 17 = UDP)**

- **Suma de verificación de cabecera: permite comprobar si la cabecera se dañó durante el transporte. No hay suma de comprobación de datos.**

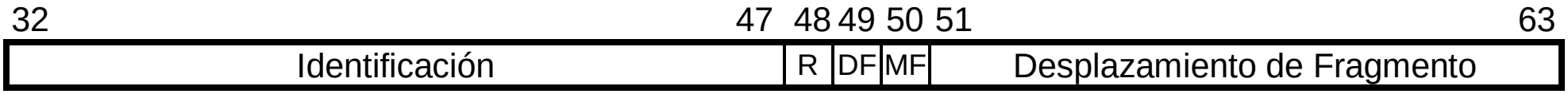
- **Dirección IP de origen: para saber de donde viene el paquete.**

- **Dirección IP destino: para que las puertas de enlace intermedias sepan hacia donde deben dirigir el paquete.**

- **Opciones IP: información adicional para controlar funciones como la seguridad y el encaminamiento (no operación, seguridad, ruta de origen desconectada, ruta de origen estricta, registro de ruta, identificador de flujo y marcas de tiempo).**

# IP (III)

**Fragmentación: los paquetes IP se deben partir cuando pasan por una red cuya unidad máxima de transferencia es menor que el tamaño del paquete.**




**Campos:**

**- Identificación: número que identifica el paquete IP.**

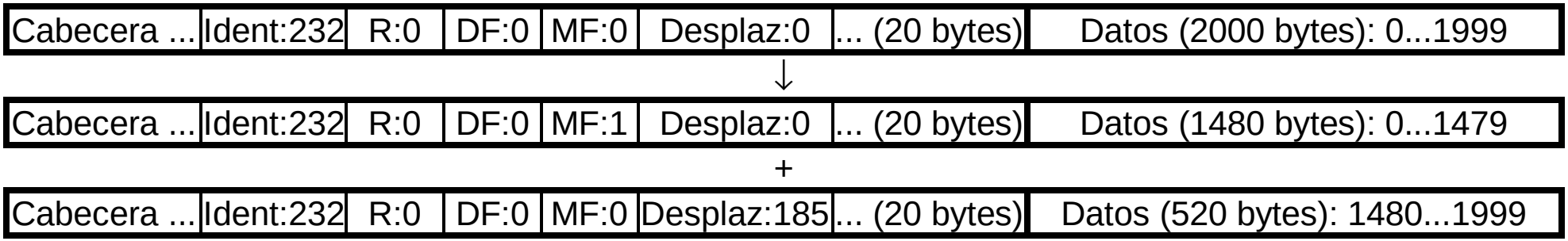
**- R: Reservado (debe ser cero).**

**- DF: 0 = se puede fragmentar, 1 = no se puede fragmentar.**

**- MF: 0 = es el último fragmento, 1 = todavía hay más fragmentos.**

**- Desplazamiento: distancia en múltiplo de 8 bytes de los datos desde el inicio del paquete.**

**Ejemplo: paquetes IP de 2020 bytes por ethernet de MTU de 1500 bytes.**



# TCP (I)[7]



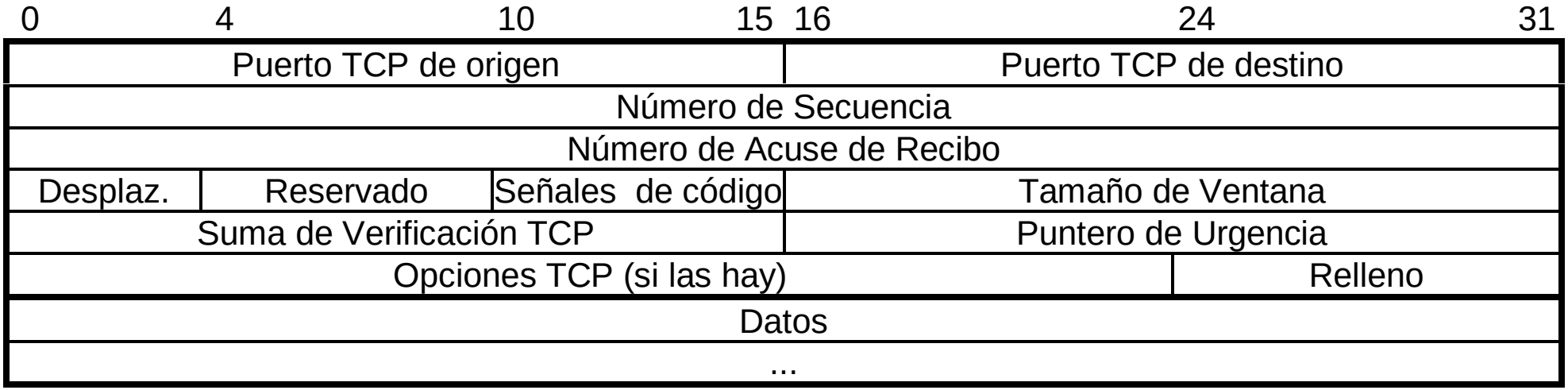
**TCP es el protocolo encargado de que la información se reconstruya de forma correcta cuando llegue a su destino, para pasarla a la aplicación.**

- **Detección y corrección de errores, cuando los datos están corruptos.**
- **Control de flujo, previniendo que el transmisor sobrepase la capacidad de recibir datos del receptor.**
- **Ordenar los datos, ya que IP puede entregar los paquetes enviados en cualquier orden.**
- **Eliminar segmentos duplicados que se han creado debido a los mecanismos de recuperación de errores de TCP.**
- **Solicitar de nuevo los segmentos que no han llegado.**


[7] http://www.faqs.org/rfcs/rfc793.html o ftp://ftp.rfc-editor.org/in-notes/rfc793.txt

# TCP (II)






- **Puertos origen y destino: identifican las aplicaciones en los extremos de la conexión, para el seguimiento de diferentes conversaciones.**

- **Número de secuencia: se utiliza para que el extremo que recibe los datagramas se asegure de colocarlos en el orden correcto y de no haber extraviado ninguno. TCP asigna un número de secuencia a cada byte transmitido, no a cada datagrama. Así, si hay 500 bytes de datos en cada datagrama, el primer datagrama será numerado 0, el segundo 500, el siguiente 1000, etc.**

- **Número de acuse de recibo: guarda el valor del siguiente número de secuencia esperado y confirma que se han recibido todos los datos a través del número de acuse de recibo menos uno. El ordenador que recibe los datos debe devolver un segmento con el bit ACK activado en el campo de código para confirmar que recibió la información. Si no lo hace antes de un cierto periodo de tiempo, se retransmiten los datos.**

- **Desplazamiento: longitud de la cabecera TCP en múltiplo de 32 bits (sin opciones = 5, con opciones = ?). Indica donde comienzan los datos.**

- **Señales de código:**
  **- URG (bit 10): El campo de puntero urgente es válido.**
  **- ACK (bit 11): El campo de acuse de recibo es válido.**
  **- PSH (bit 12): El receptor no pondrá en cola los datos, sino que los pasará inmediatamente a la aplicación.**
  **- RST (bit 13): Destruir la conexión.**
  **- SYN (bit 14): Iniciar la conexión - Sincronizar los números de secuencia.**
  **- FIN (bit 15): Finalizar la conexión - El emisor ha llegado al final de su flujo de datos.**

- **Tamaño de ventana: se utiliza para controlar cuanta información puede estar en tránsito en un momento dado. Cada extremo indica en este**

**campo cuantos bytes de datos nuevos está actualmente preparado para aceptar.**

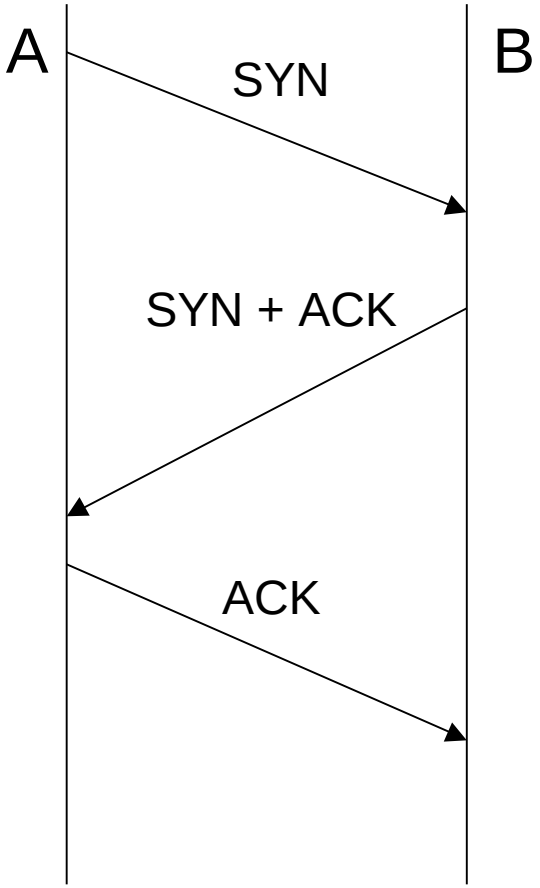
- **Suma de verificación TCP: permite comprobar si la cabecera y los datos se dañaron durante el transporte. Si la suma de todos los bytes del datagrama recibido no coincide con la de este campo, no se envía el segmento ACK de confirmación y los datos son reenviados**

- **Puntero de urgencia: posición de los datos que deben ser procesados primero.**

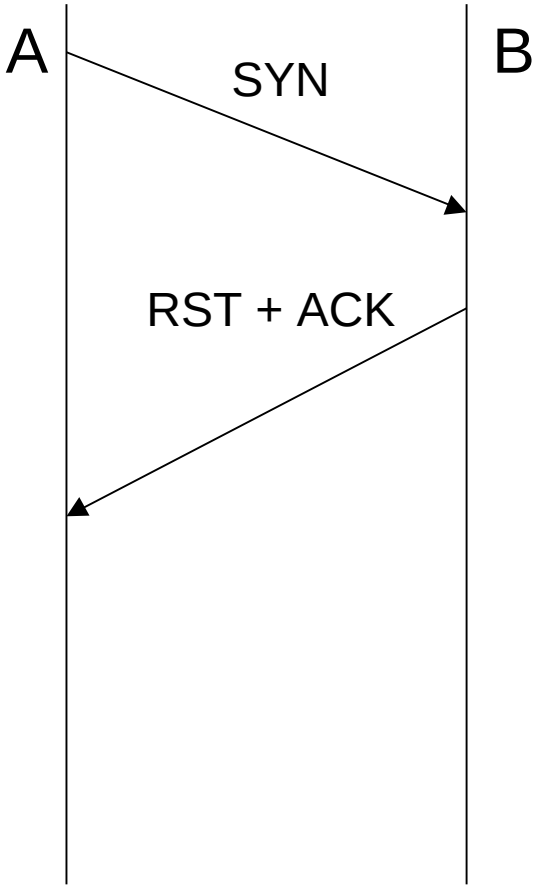
- **Opciones TCP: información adicional (tamaño máximo de segmento, escala de ventana, marca de tiempo, no operación (NOP), acuse de recibo selectivo, acuse de recibo selectivo permitido (SackOK) y datos del acuse de recibo selectivo).**

# TCP (III)

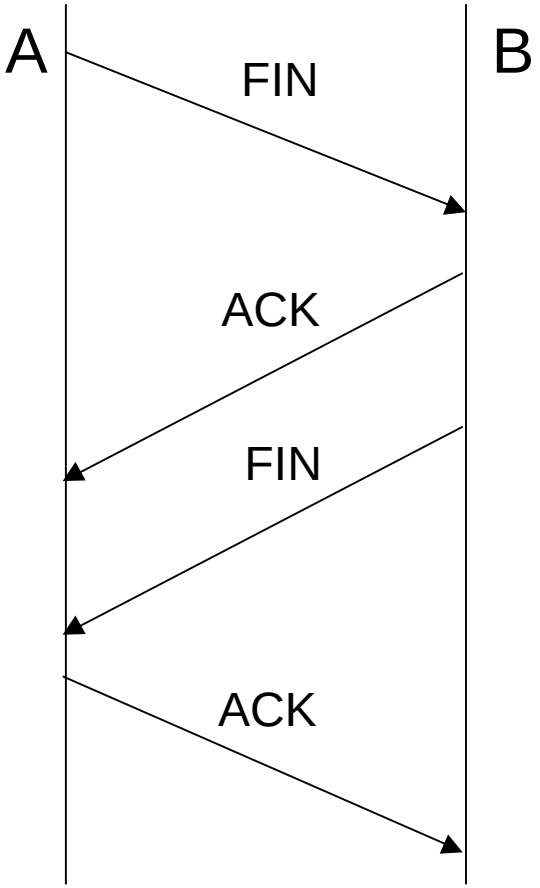
## Establecimiento de conexión (puerto abierto)



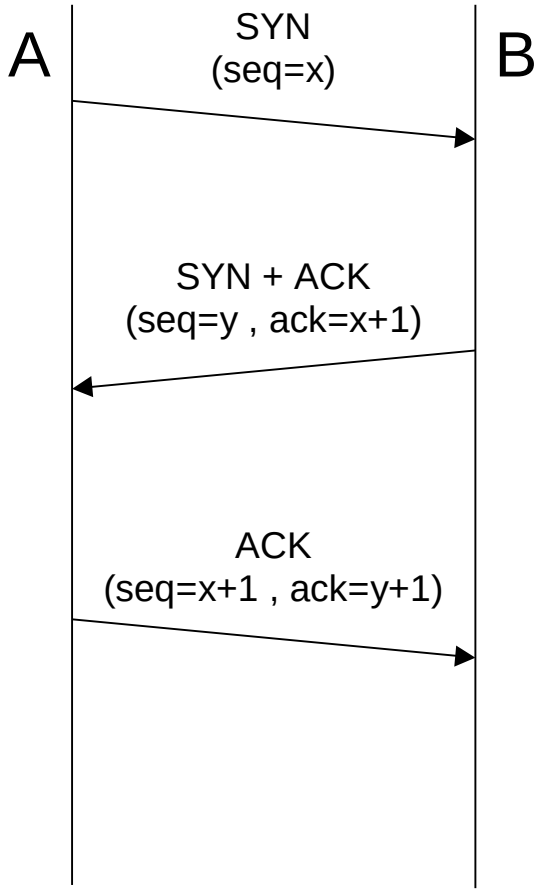

## Establecimiento de conexión (puerto cerrado)



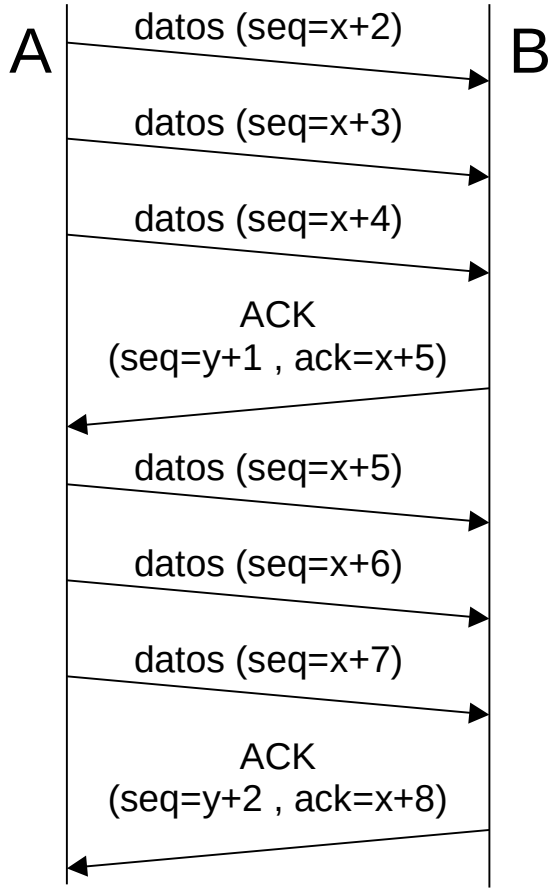

## Cierre de la conexión



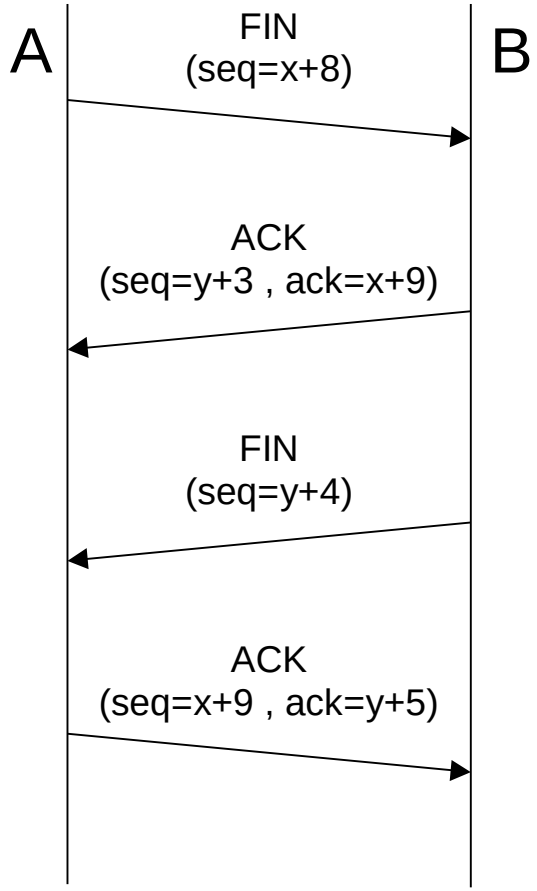
## Establecimiento de la conexión




## Envío de la información (6 paquetes, ventana = 3)




## Cierre de la conexión



# UDP (I)[8]



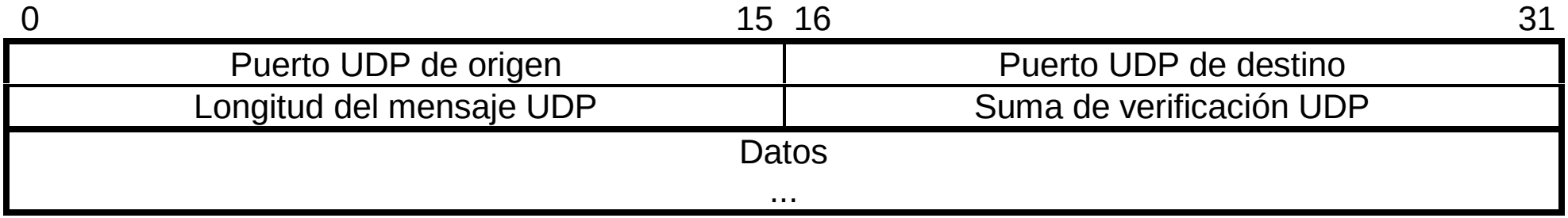
**UDP es un protocolo alternativo a TCP, que se utiliza cuando se desea enviar pocos datos rápidamente, sin tener en cuenta si llegan a su destino o no.**

- **Aplicaciones donde no es esencial que lleguen el 100% de los paquetes (como el flujo de sonido o vídeo).**
- **Los mensajes caben en un solo paquete (por ejemplo los protocolos DNS, RPC, NFS, SNMP) y no es necesaria la complejidad de TCP (si no se obtiene respuesta pasados unos segundos, se vuelve a enviar).**


[8] http://www.faqs.org/rfcs/rfc768.html o ftp://ftp.rfc-editor.org/in-notes/rfc768.txt

# UDP (II)






- **Puertos origen y destino: identifican las aplicaciones en los extremos de la conexión, para el seguimiento de diferentes conversaciones.**
- **Longitud: longitud en bytes del paquete UDP (incluyendo la cabecera).**
- **Suma de verificación: permite comprobar si la cabecera y los datos se dañaron durante el transporte.**

# CONTRASTES TCP/UDP



**TCP (más seguro)**

- **Genera una conexión previa al intercambio de datos.**
- **Conexión punto a punto.**
- **Realiza suma de comprobación de los datos.**
- **Los paquetes de datos tienen un número. Cuando son recibidos se ordenan para entregarlos a la aplicación. Se envían confirmaciones de que los paquetes han llegado a su destino. Si el envío falla se reenvían.**

**UDP (más rápido)**

- **Envía los datos “sin avisar”.**
- **Puede realizar broadcast.**
- **Puede realizar suma de comprobación de los datos.**
- **Confía en que los paquetes de datos lleguen.**

# ICMP (I)[9]



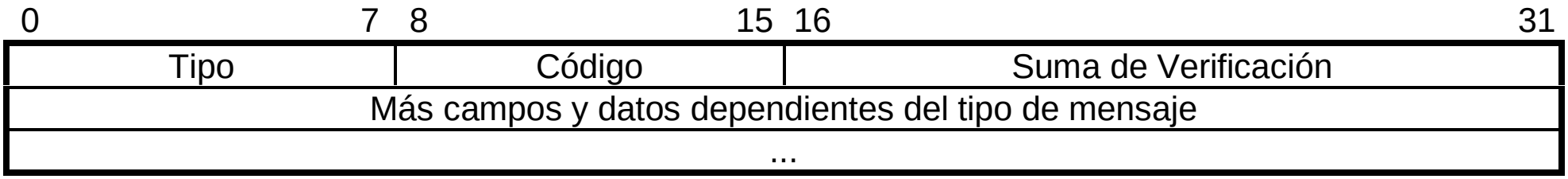
**Son mensajes de error que ayudan al nivel IP:**

- **Un problema de transmisión en un nodo genera un mensaje ICMP (se excedió el tiempo de vida del paquete, no se alcanzó el destino, ...).**
- **También se utiliza para diagnosticar el funcionamiento de la red (ping, traceroute, ...).**
- **Los mensajes de error no se generan ni en direcciones broadcast/multicast, ni cuando se produce un error dentro del mismo mensaje de error.**


[9] http://www.faqs.org/rfcs/rfc792.html o ftp://ftp.rfc-editor.org/in-notes/rfc792.txt

# ICMP (II)






- **Tipo: tipo de mensaje ICMP.**
- **Código: subtipo de mensaje ICMP (información más detallada del tipo).**
- **Suma de verificación: permite comprobar si la cabecera y los datos se dañaron durante el transporte.**

| tipo | código | significado |
|---|---|---|
| 0 | 0 | Respuesta de eco |
| 3 | 0 | Red inalcanzable |
| 3 | 1 | Equipo inalcanzable |
| 3 | 3 | puerto inalcanzable |
| 8 | 0 | Solicitud de eco |
| 11 | 0 | Tiempo excedido para un datagrama |

# IPv6 (I)[10]



**Limitaciones de IPv4:**

- **El espacio de direcciones IPv4 quedará exhausto entre 2005 y 2011.**
- **Tablas de encaminamiento cada vez más grandes.**
- **Necesidad de nuevas características: multimedia, seguridad, ...**
- **Oportunidad de implementar mejoras que han ido apareciendo.**

**Ventajas de IPv6 (que es compatible con IPv4):**

- **Mayor espacio de direcciones: 128 bits.**
- **Soporte para tiempo real.**
- **Autoconfiguración de estaciones de trabajo.**
- **Seguridad.**

[10] http://www.faqs.org/rfcs/rfc2460.html o ftp://ftp.rfc-editor.org/in-notes/rfc2460.txt

# IPv6 (II)



**En IPv6, la dirección IP tiene una longitud de 128 bits, expresada como ocho números hexadecimales de dos bytes separados por dos puntos.**

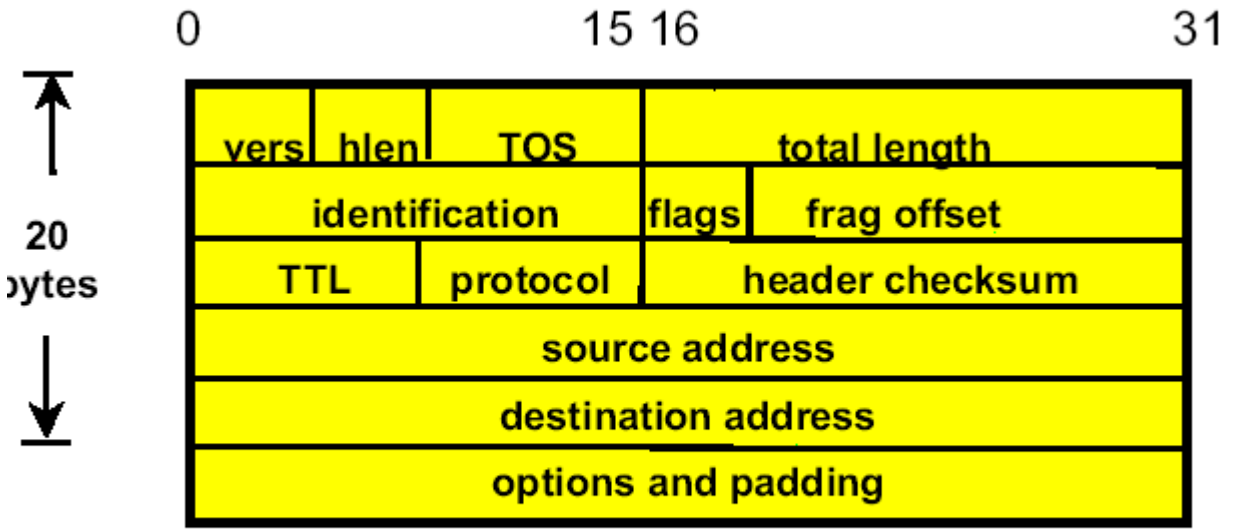
Por ejemplo: 1080:0:0:0:8:800:200C:417A $\Rightarrow$ 1080::8:800:200C:417A

- **Unicast: Representa un interfaz de red. Cada paquete enviado a una dirección unicast se entrega a la interfaz identificada por esa dirección.**
- **Anycast: Representa un conjunto de interfaces de red. Cada paquete enviado a una dirección anycast se entrega a una de las interfaces.**
- **Multicast: Representa un conjunto de interfaces de red. Cada paquete enviado a una dirección multicast se entrega a todas las interfaces.**

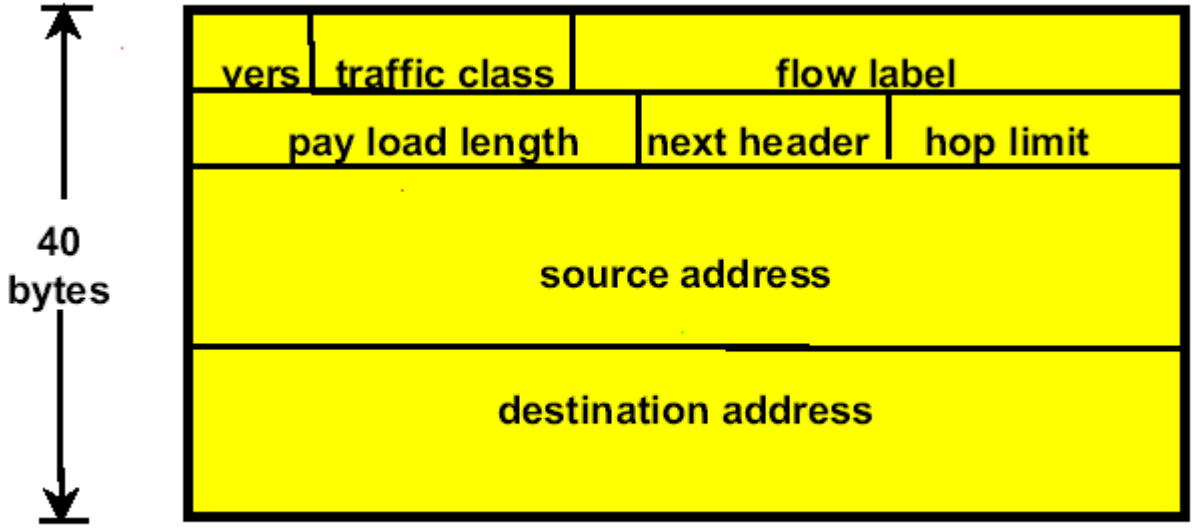
# IPv6 (III)



- **Eliminado:**
  **ID, flags, frag offset, TOS, hlen y header checksum.**
- **Cambiado:**
  **total length ® payload, protocol ® next header y TTL ® hop limit.**
- **Añadido:**
  **trafic class y flow label.**
- **Expandido:**
  **direcciones de 32 bits a 128 bits.**




IPv4




IPv6

# IPv6 (IV)



**Autoconfiguración:**

- **Estática: prefijo router (4c00::/80) + dirección tarjeta de red (00:A0:C9:1E:A5:B6) = dirección IPv6 (4c00::00:A0:C9:1E:A5:B6).**
- **Dinámica: solicitud DHCP enviando dirección tarjeta de red (00:A0:C9:1E:A5:B6) => respuesta DHCP (4c00::00:A0:C9:1E:A5:B6).**

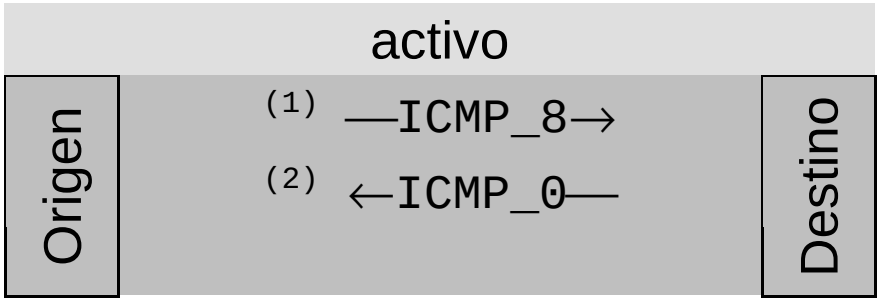
**Seguridad:**

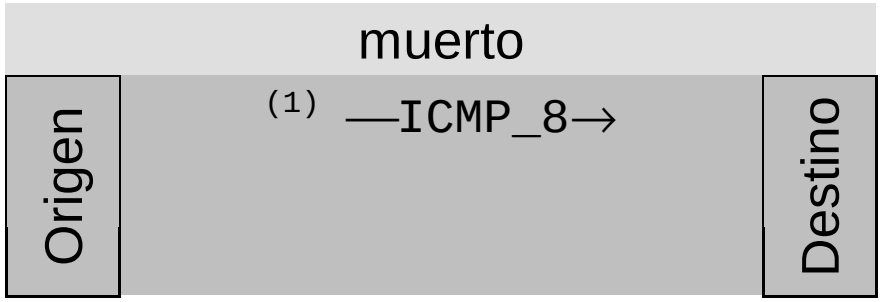
- **Autenticación: MD5.**
- **Confidencialidad: DES-CBC + encriptación del payload.**

**Migración IPv4 a IPv6:**

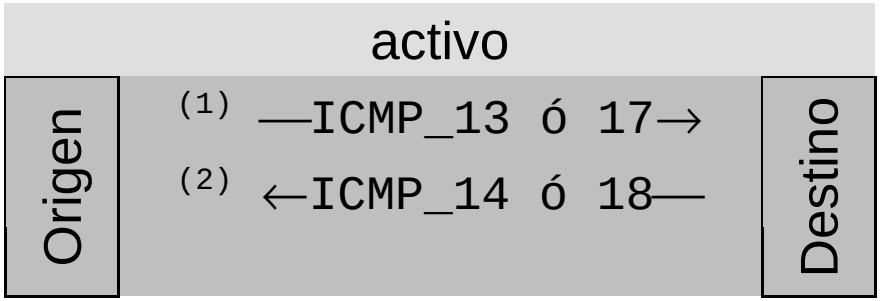
1. **Actualizar los servidores de DNS para que manipulen direcciones IPv6.**
2. **Introducir sistemas con pilas duales, que soporten IPv4 e IPv6.**
3. **Conectar redes IPv6 separadas por redes IPv4 a través de tuneles.**
4. **Eliminar el soporte para IPv4.**
5. **Utilizar traslación de cabeceras para sistemas que sólo utilicen IPv4.**

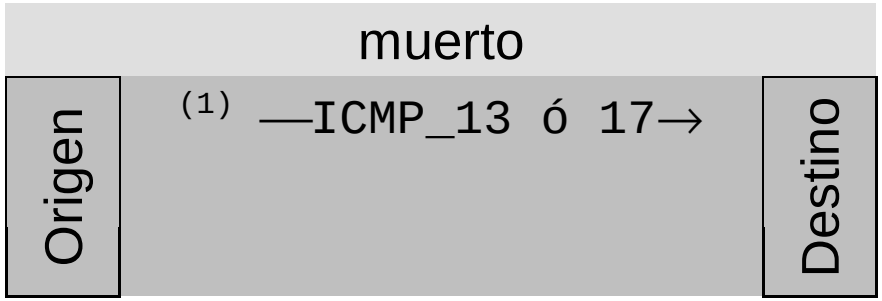
- **Echo ICMP.**



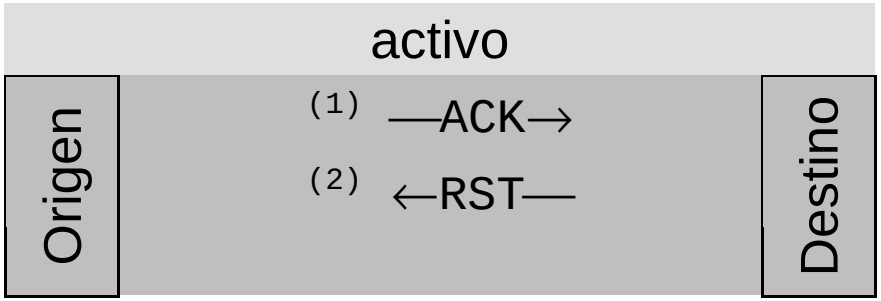

- **Non-Echo ICMP.**

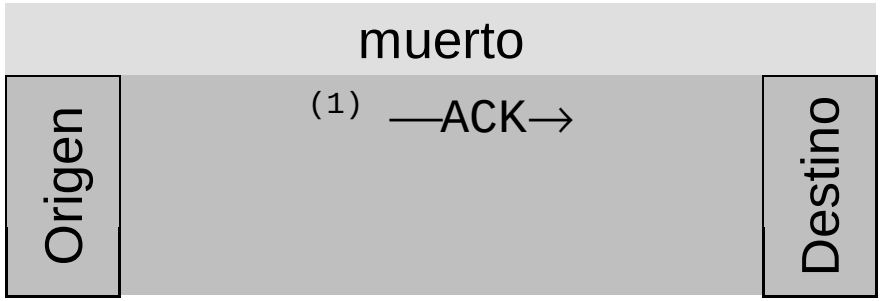


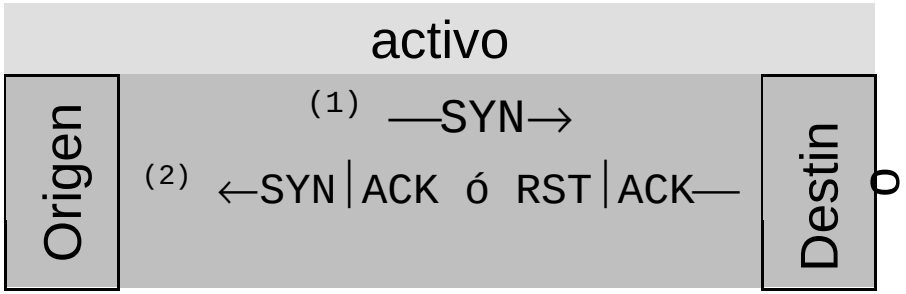




- **Broadcast ICMP: lo mismo, pero dirigido a la dirección de broadcast.**

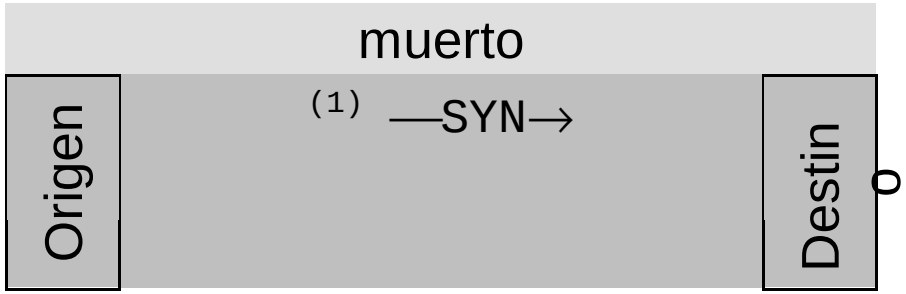
- **TCP sweeps.**



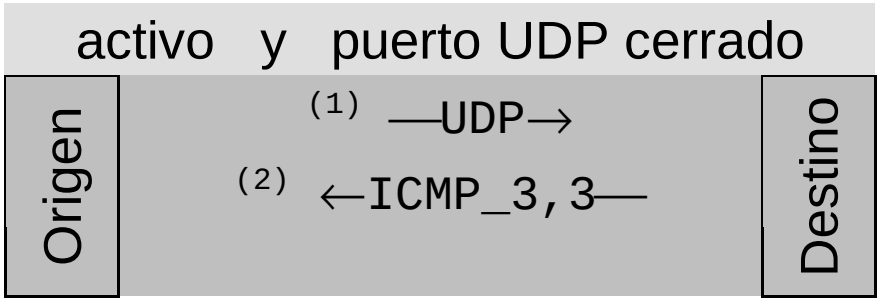



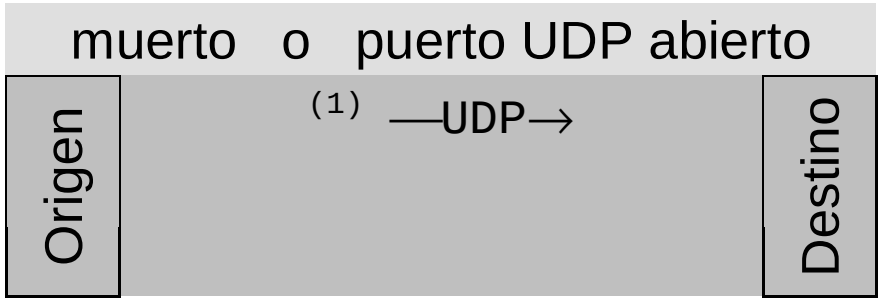

o



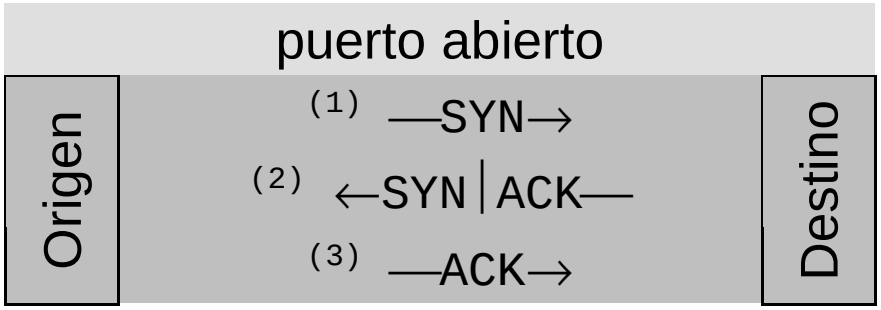

o

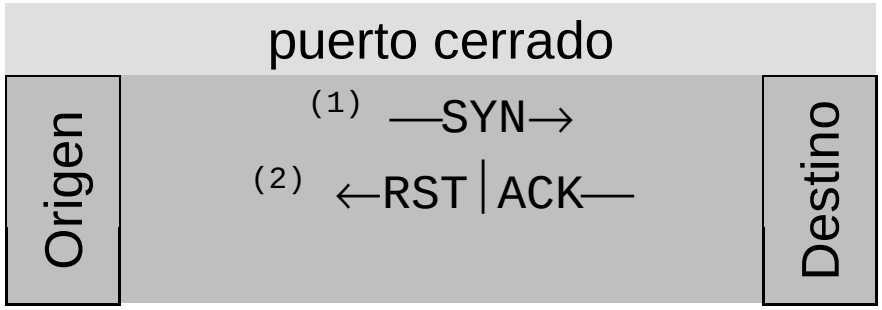
- **UDP sweeps.**



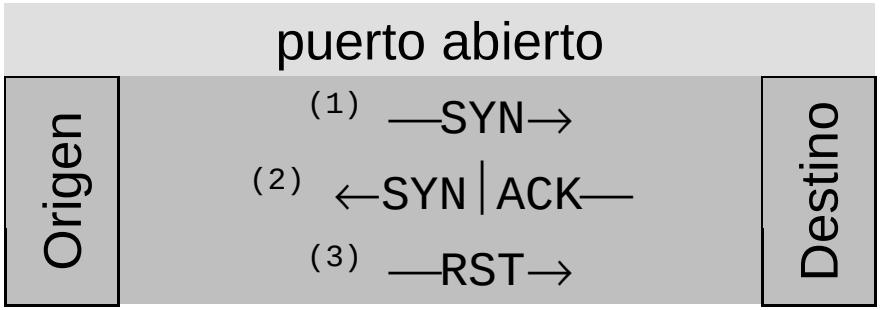



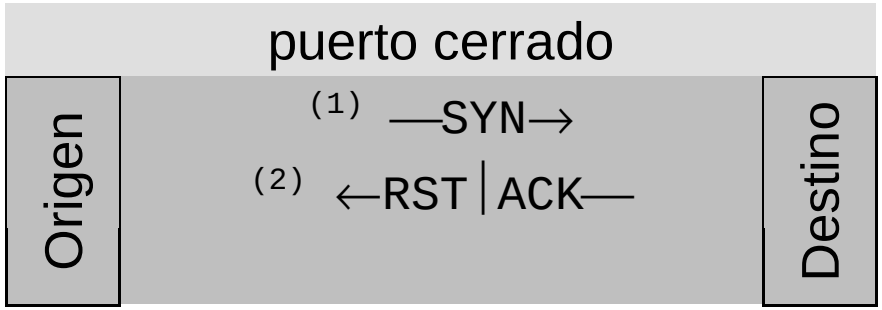
- **TCP connect() scan.**



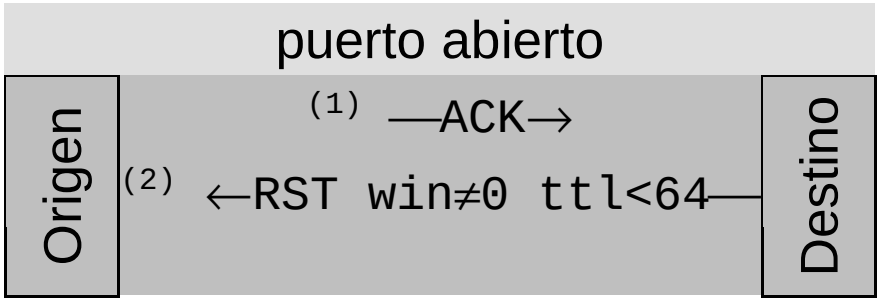



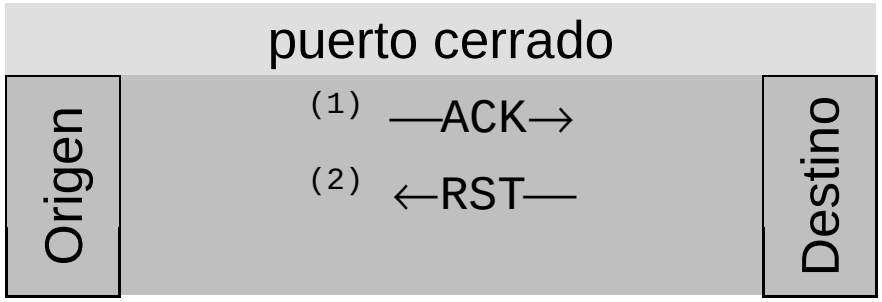

- **TCP SYN scan.**



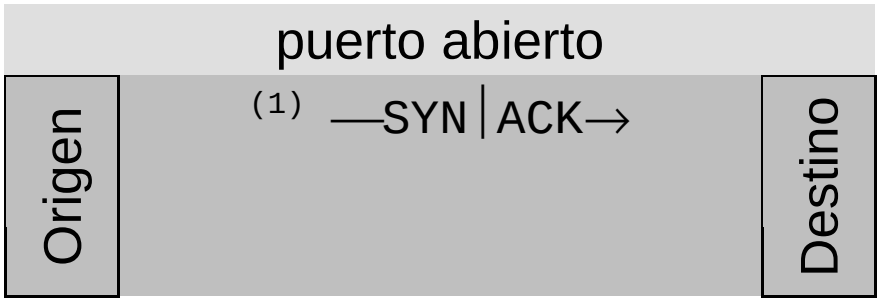



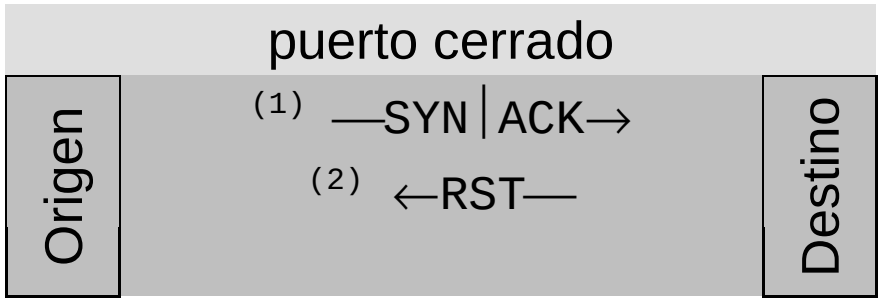
- **TCP ACK scan.**



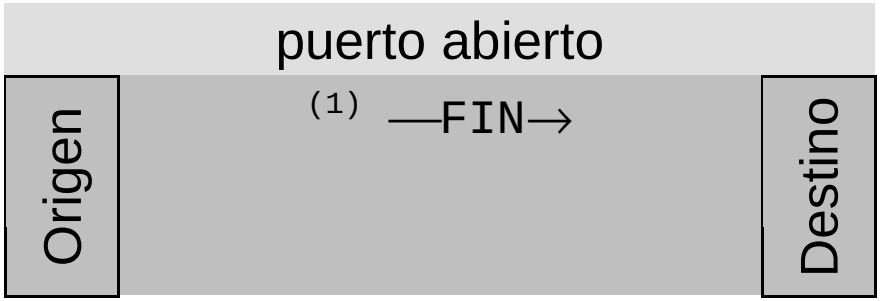



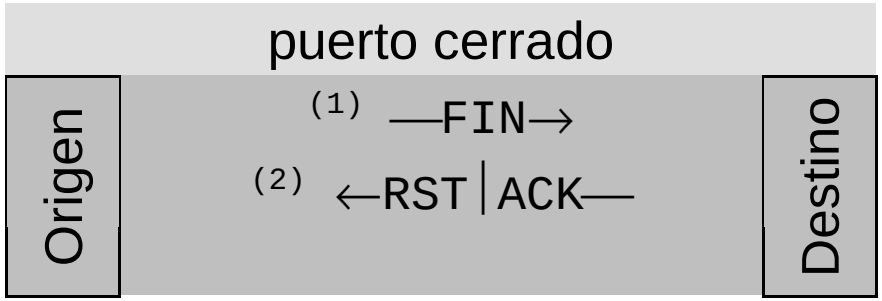

- **TCP SYN|ACK scan.**



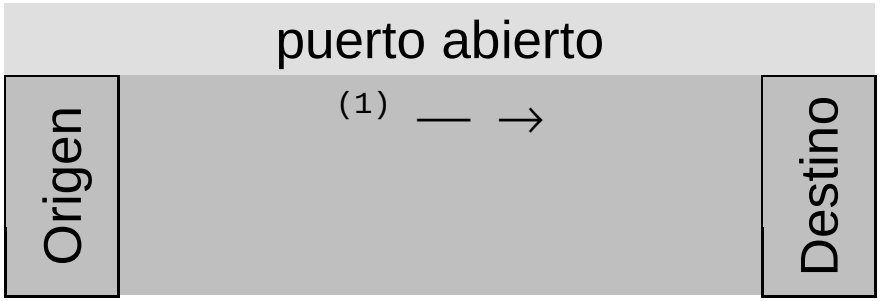



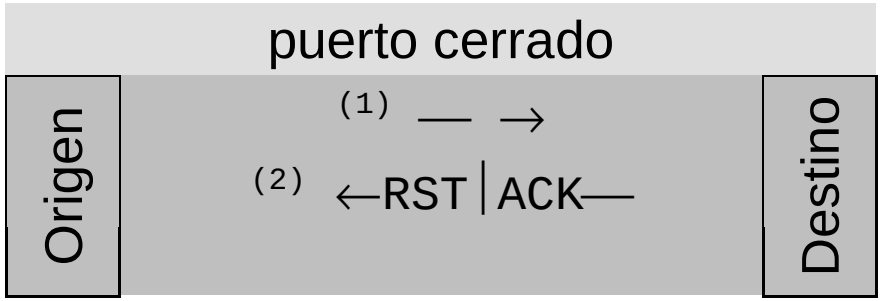

- **TCP FIN scan.**



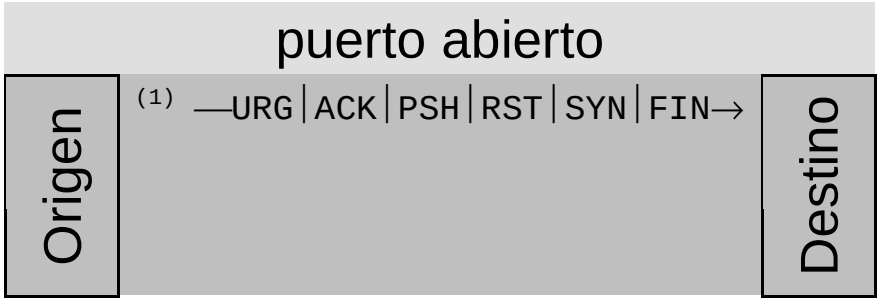



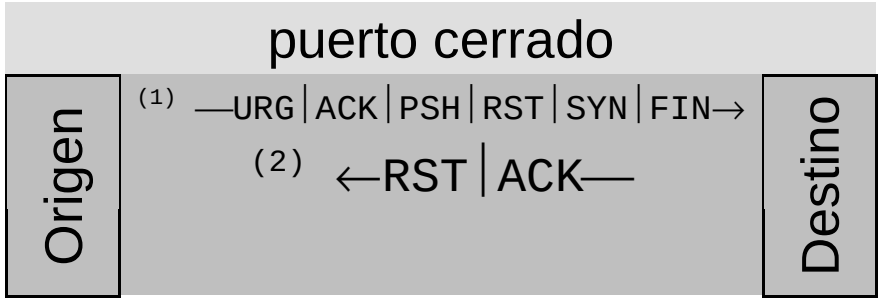
- **TCP Null scan.**



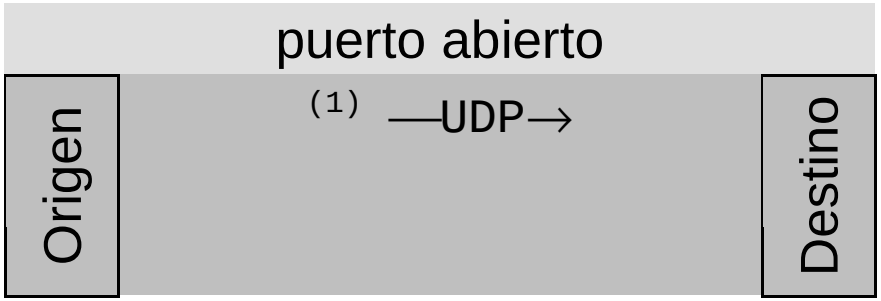



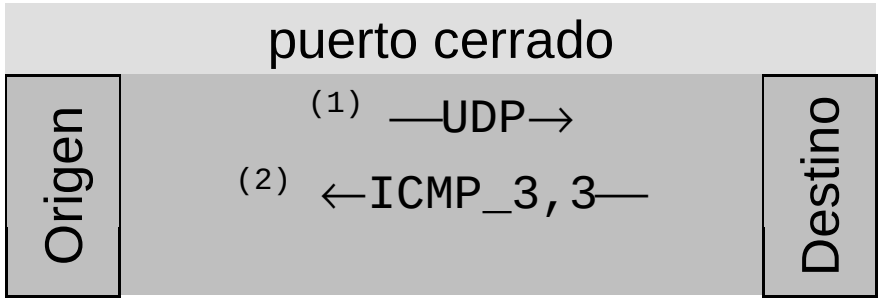

- **TCP Xmas scan.**



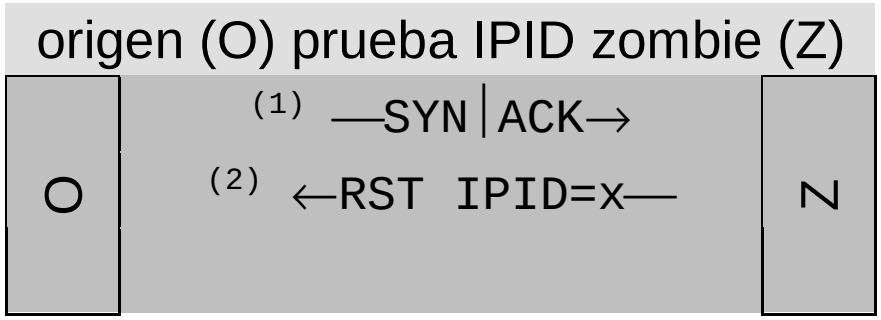



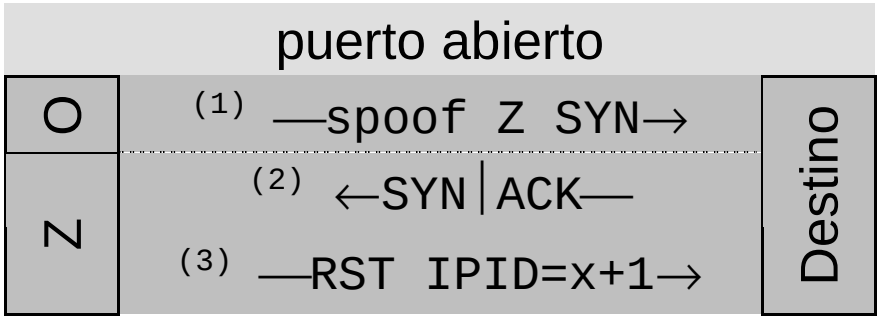

- **UDP ICMP port unreachable scan + recvfrom() and write() scan.**

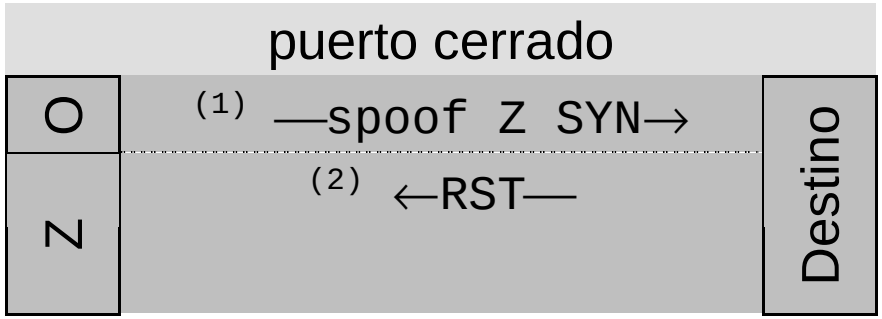


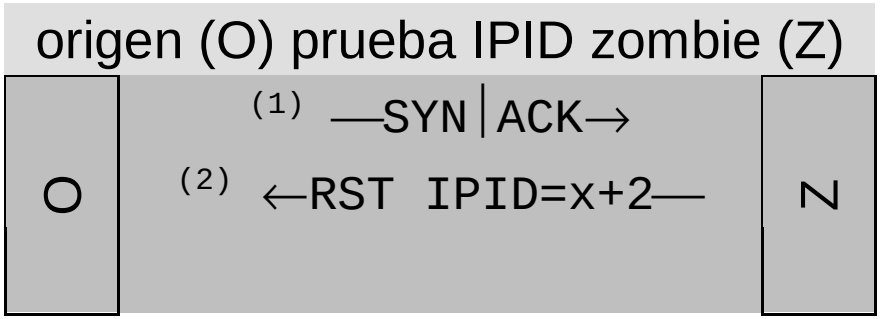



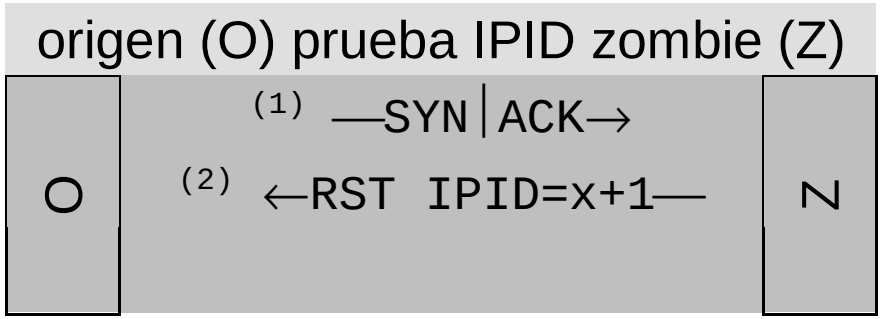
- **Dumb host scan.**



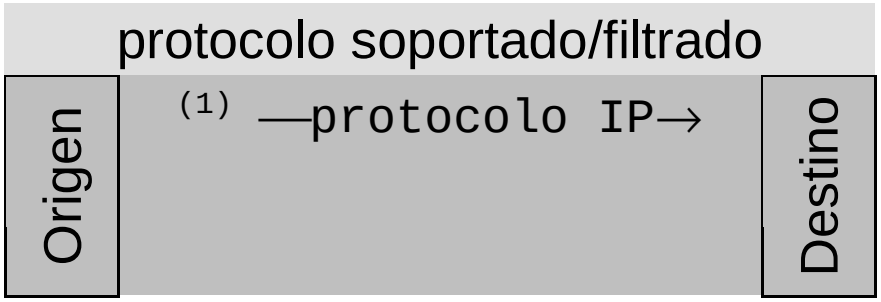



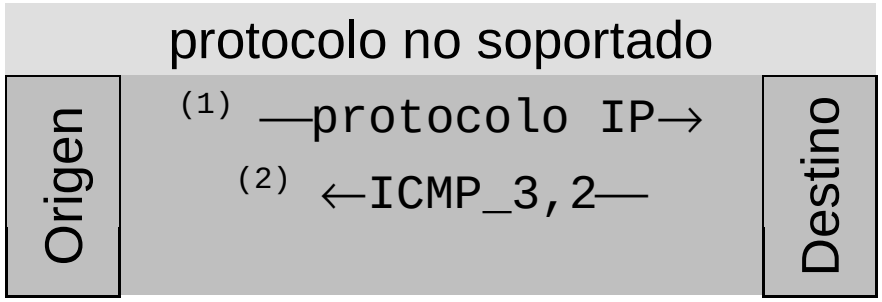



- **TCP reverse ident scan:** El protocolo IDENT (puerto 113) permite descubrir el nombre del usuario propietario de los procesos conectados mediante TCP.

- **IP protocol scan:** TCP, UDP, ICMP, IGMP, IGP, EGP, GRE, SWIPE, NARP, MOBILE, SUN-ND, EIGRP, OSPFIGP, IPIP, PIM, etc.



- **Ejemplo de análisis horizontal (logs de Snort):**
  **Caso típico en el que un atacante tiene un exploit para un servicio y analiza todos los ordenadores de una red para ver si tienen abierto el puerto asociado a dicho servicio.**

```
Apr 1 19:02:12 66.66.66.66:1078 -> 11.11.11.197:53 SYN
Apr 1 19:02:12 66.66.66.66:1079 -> 11.11.11.198:53 SYN
Apr 1 19:02:12 66.66.66.66:1080 -> 11.11.11.199:53 SYN
Apr 1 19:02:12 66.66.66.66:1081 -> 11.11.11.200:53 SYN
Apr 1 19:02:12 66.66.66.66:1082 -> 11.11.11.201:53 SYN
Apr 1 19:02:12 66.66.66.66:1083 -> 11.11.11.202:53 SYN
```

- **Ejemplo de análisis vertical (logs de Snort):**
  **Caso típico en el que un atacante quiere comprometer la seguridad de una máquina en particular y analiza los puertos de dicha máquina para saber cuales están abiertos y cuales no.**

```
Apr 1 19:36:01 66.66.66.66:1093 -> 11.11.11.49:21 SYN
Apr 1 19:36:01 66.66.66.66:1094 -> 11.11.11.49:23 SYN
Apr 1 19:36:01 66.66.66.66:1095 -> 11.11.11.49:25 SYN
Apr 1 19:36:02 66.66.66.66:1096 -> 11.11.11.49:53 SYN
Apr 1 19:36:02 66.66.66.66:1096 -> 11.11.11.49:79 SYN
Apr 1 19:36:02 66.66.66.66:1097 -> 11.11.11.49:80 SYN
```

- **FIN probe.**
- **BOGUS flag probe.**
- **TCP ISN Sampling.**
- **IPID Sampling.**
- **TCP Timestamp.**
- **Don’t Fragment bit.**
- **TCP Initial Window.**
- **ACK value.**
- **ICMP error message quenching.**
- **ICMP message quoting.**
- **ICMP error message echoing integrity.**

- **Type of Service.**
- **Fragmentation Handling.**
- **TCP Options.**
- **Retransmission Timeout.**
- **Port 0 probe.**
- **Exploit chronology.**
- **SYN Flood resistance.**

- **Análisis al azar de puertos.**
- **Análisis lento.**
- **Análisis distribuido.**
- **Fragmentación de paquetes.**
- **Análisis a través de proxy.**
- **Análisis con señuelos.**

## ANÁLISIS PASIVO (I)

**El análisis pasivo no consiste en enviar información al ordenador a analizar, sino en esperar a recibirla cuando éste establece una conexión a nuestro ordenador.**

**Los paquetes capturados contienen suficiente información para determinar el sistema operativo con que funciona: tiempo inicial de vida, tamaño de ventana, tamaño máximo de segmento, bit de no fragmentación, opción sackOK, opción NOP, opción de escalado de ventana ... ( una firma de 51 bits para cada sistema operativo.**
**Existen todavía numerosos campos y valores a explorar: números iniciales de secuencia, números de identificación IP, opciones TCP e IP, TOS, ...**

**A nivel de aplicación:**
**- clientes de correo electrónico: adjuntan información del usuario en el campo X-Mailer de la cabecera.**
**- peticiones de páginas web de los navegadores: adjuntan información en los campos User-Agent, Host y Server de la cabecera.**
**- clientes telnet: cada cliente negocia la velocidad de línea, el tipo de terminal y el eco de manera diferente.**

## ANÁLISIS PASIVO (II)

**Ventajas:**

- **Imposible de detectar. No envía información.**
- **Permite descubrir ordenadores que están activos durante un breve lapso de tiempo.**
- **Permite descubrir servicios ocultos.**

**Limitaciones:**

- **Es poco específico. Se debe esperar un intento de conexión.**
- **Errores analizando los paquetes de un análisis activo.**
- **Es fácil alterar los parámetros que son observados por un análisis pasivo.**

# ANÁLISIS PASIVO (III)

**Usos:**

**Atacantes pueden determinar el sistema operativo de una víctima en potencia, como por ejemplo un servidor de páginas web, solicitando una página de dicho servidor, que es una conducta normal que no levantará sospechas, y analizando después los rastros del sniffer.**

**Organizaciones pueden inventariar rápidamente los sistemas operativos de los ordenadores de sus redes sin alterar el rendimiento de dichas redes, e identificar sistemas no autorizados.**

**Los sistemas de detección de intrusos pueden incorporar herramientas de análisis pasivo para detectar el sistema operativo de las máquinas que han realizado un análisis activo sobre un sistema.**

**Escuchando el tráfico en puntos críticos o de choque de Internet, se pueden utilizar los datos obtenidos para mapear lentamente las redes donde se dirigen los usuarios y las redes de donde vienen solicitudes de servicios. Una red grande y distribuida de filtros puede obtener mapas de redes de calidad.**

- **Tríptico “TCP/IP pocket reference guide”:**
  http://www.sans.org/resources/tcpip.pdf
- **Transparencias “TCP/IP”:**
  http://www.cpe.ku.ac.th/~nguan/resource/slide/network.html
- **Película “Warriors of the net”:**
  http://www.warriorsofthe.net/movie.html
- **Documento “Análisis activo y pasivo de redes”:**
  http://www.xtec.net/~acastan/textos/
- **Documento “Análisis de seguridad de la familia de protocolos TCP/IP y sus servicios asociados”:**
  http://es.tldp.org/Manuales-LuCAS/doc-seguridad-tcpip/Seguridad_en_TCP-IP_Ed1.pdf
- **Documento “Security Problems with the Internet Architecture”:**
  http://ocw.mit.edu/NR/rdonlyres/Electrical-Engineering-and-Computer-Science/6-829Computer-NetworksFall2002/7C9AFDED-F5A3-406F-A685-09E5FD1B9F0B/0/L7Security.pdf