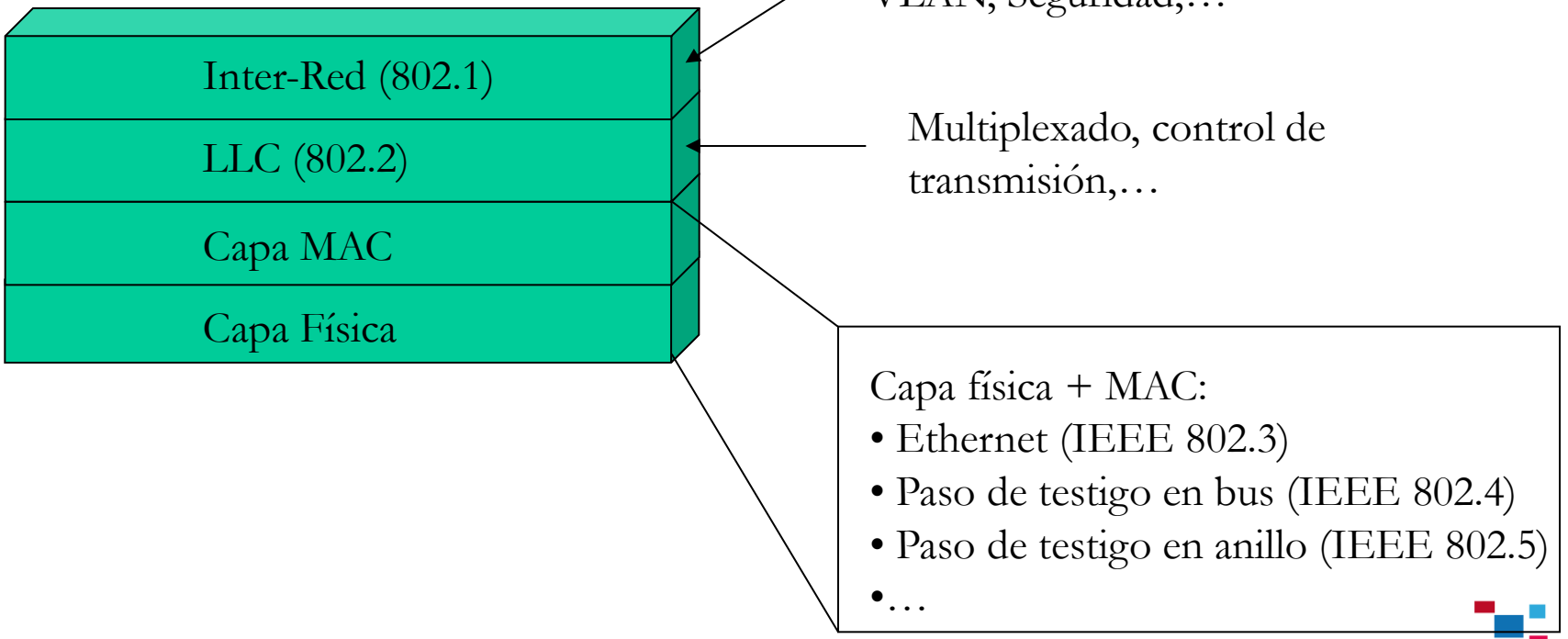
Ethernet y TCP/IP

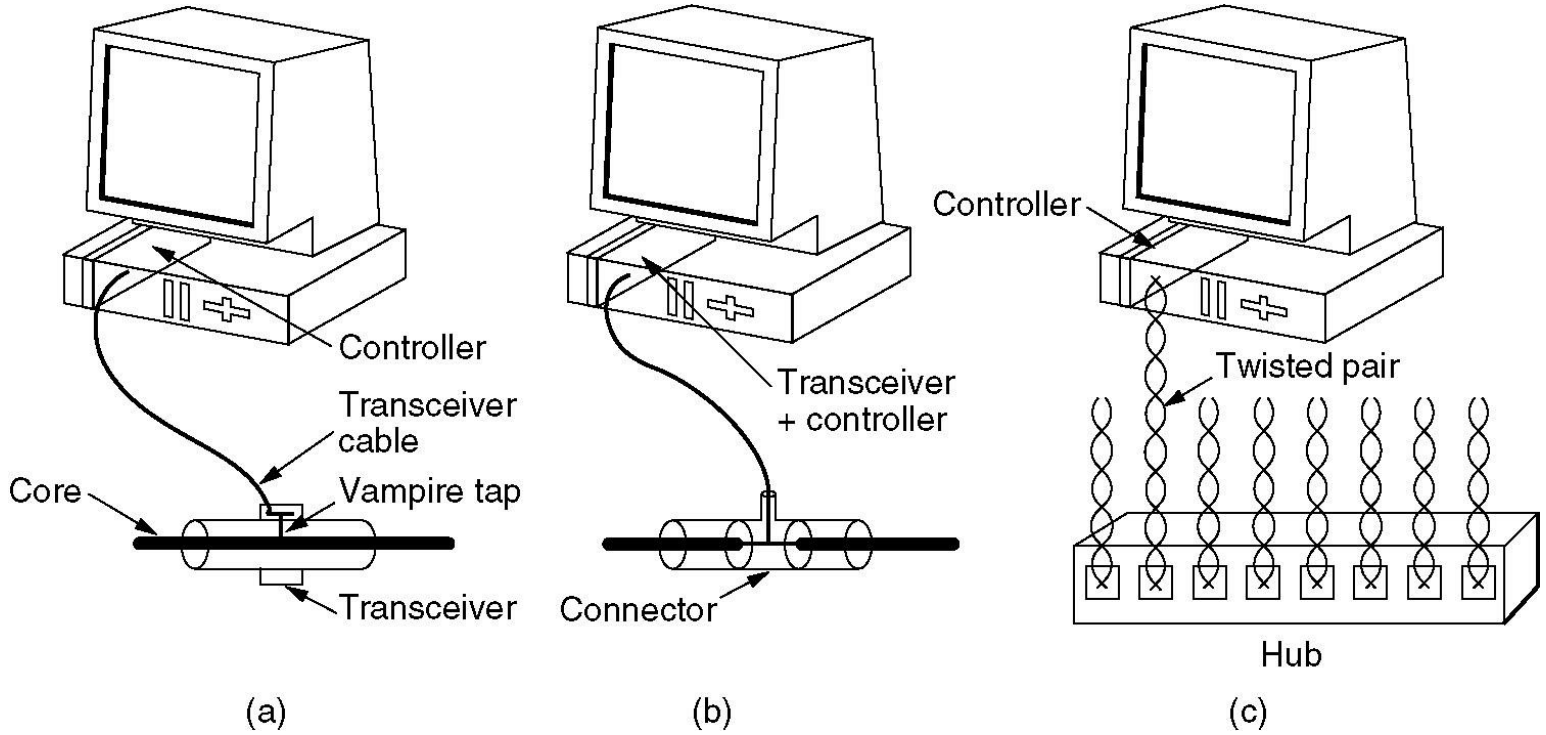
La norma IEEE 802 para redes locales



Capa Física (I)

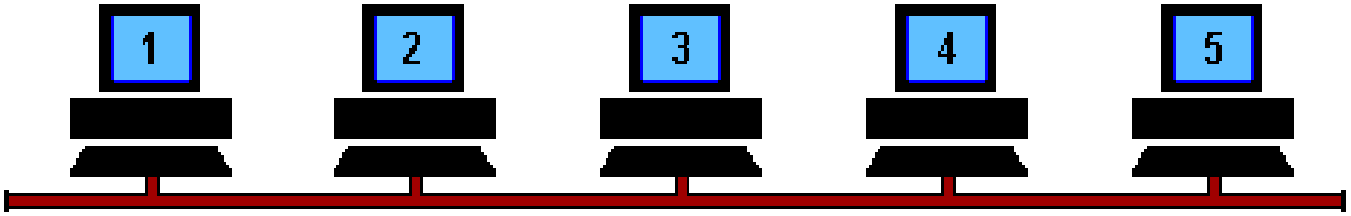
	10-Base-5	10-Base-2	10-Base-T	10-Base-F
Velocidad	10 Mbps	10 Mbps	10 Mbps	10 Mbps
Longitud del segmento	500 m. (max)	185 m. (max)	100 m. (max)	1 km.(max)
Nodos por segmento	100 (max)	30 (max)	1	1
Longitud entre nodos	2.5 (min)	0.5 (min)	--	--
Cable	Coaxial Ø 0.4 in. 75 Ω Malla doble	Coaxial Ø 0.2 in. 50 Ω Malla simple	Par trenzado Con o sin malla	Fibra óptica

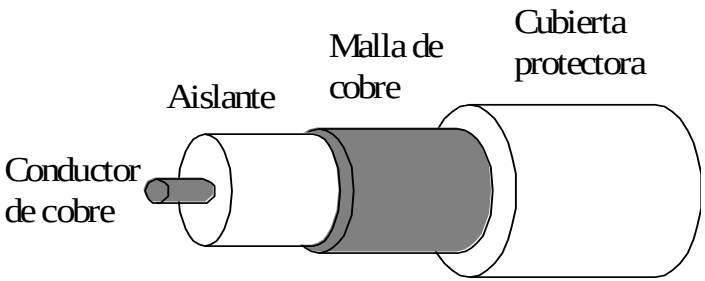
Capa Física (y II)



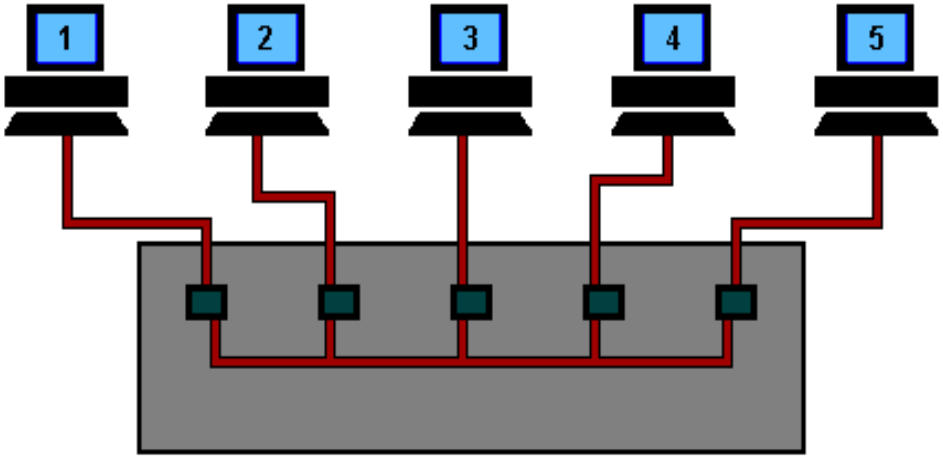
(a) 10Base5, (b) 10Base2, (c) 10Base-T.

Subcapa MAC: CSMA/CD

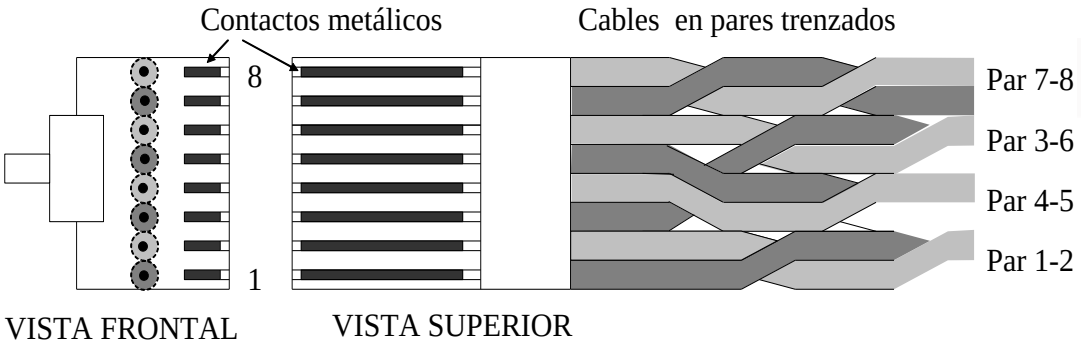




Subcapa MAC: CSMA/CD

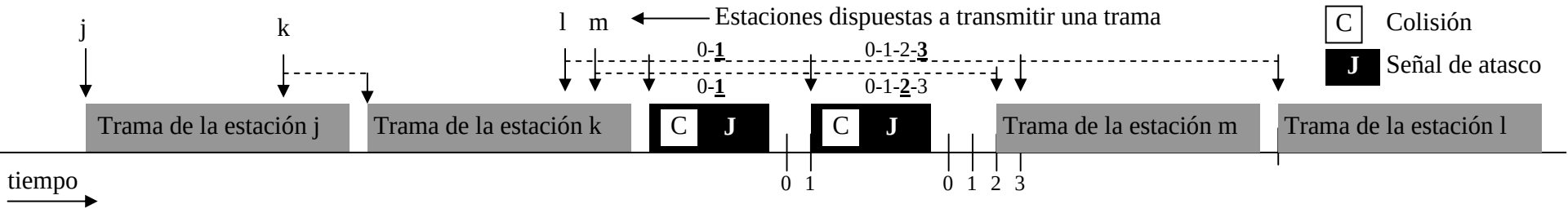


CONECTOR RJ-45

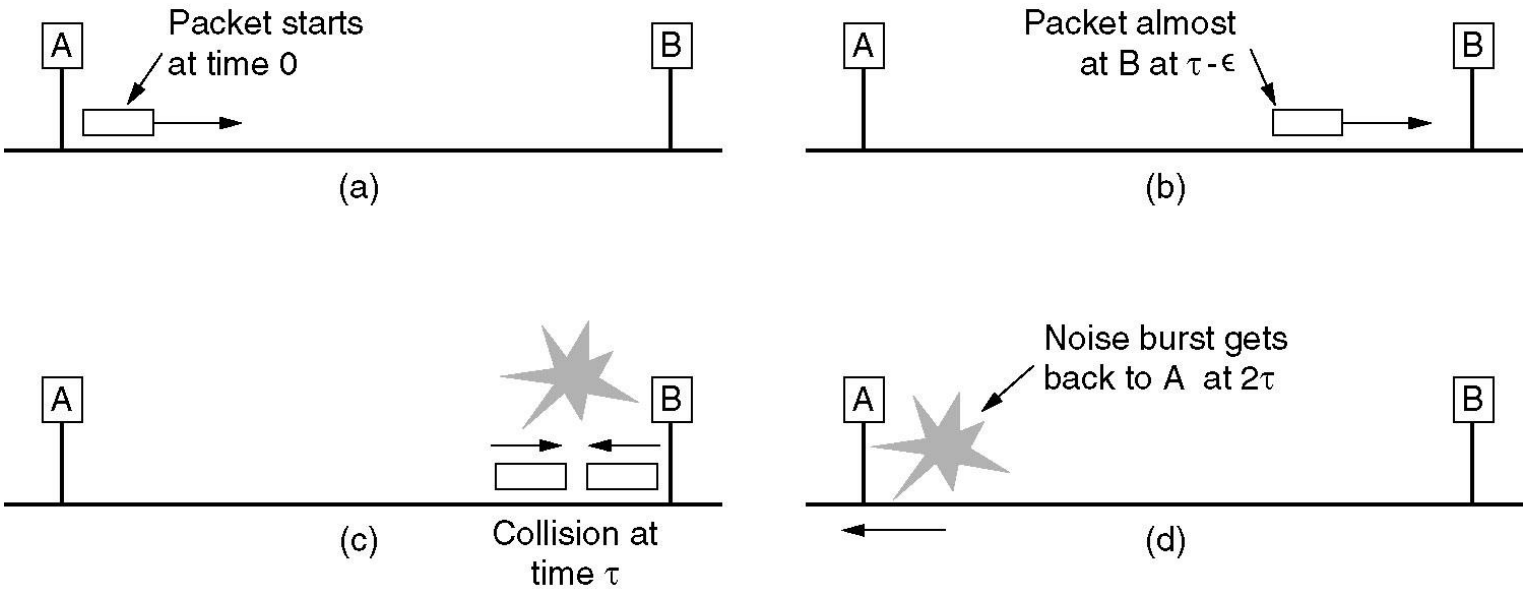


Subcapa MAC: CSMA/CD

- Control acceso al medio CSMA 1-P con detección de colisiones
- Señalización de colisiones mediante señal de "*jamming*" (atasco)
- Algoritmo de "disminución exponencial binaria"
- Problemática en aplicaciones en tiempo real
- Limitaciones de tamaño debidas a la "ventana de colisión"

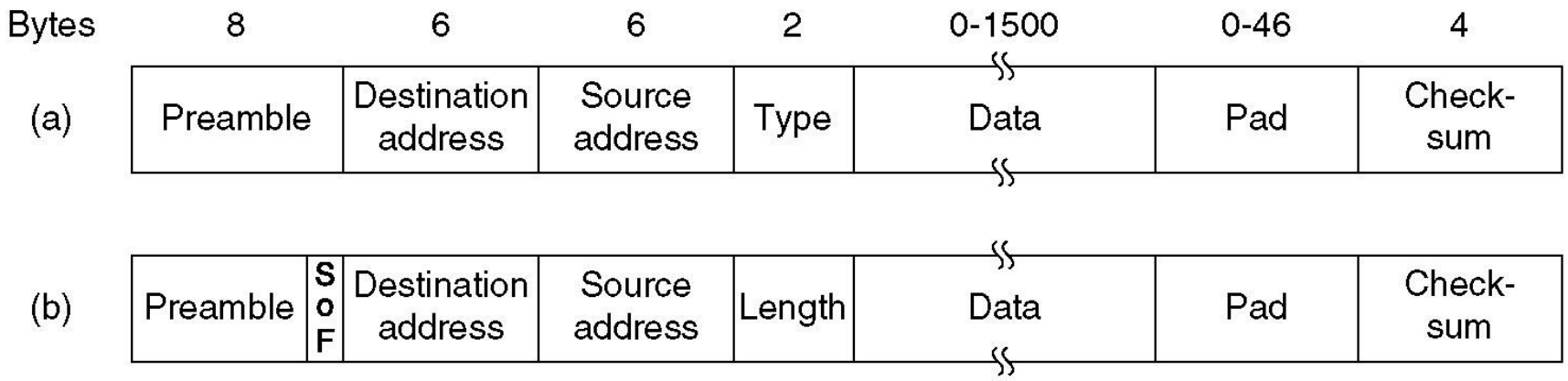


La Ventana de Colisión



- En el peor caso (2500 metros y 4 repetidores, según IEEE 802.3) a 10 Mbps, la trama debe ser > 500 bits para que lleve más de 2τ (evitar *late collisions*).
- Se redondea a 512 bits (64 bytes)

Formato de la trama Ethernet



(a) DIX Ethernet, (b) IEEE 802.3.

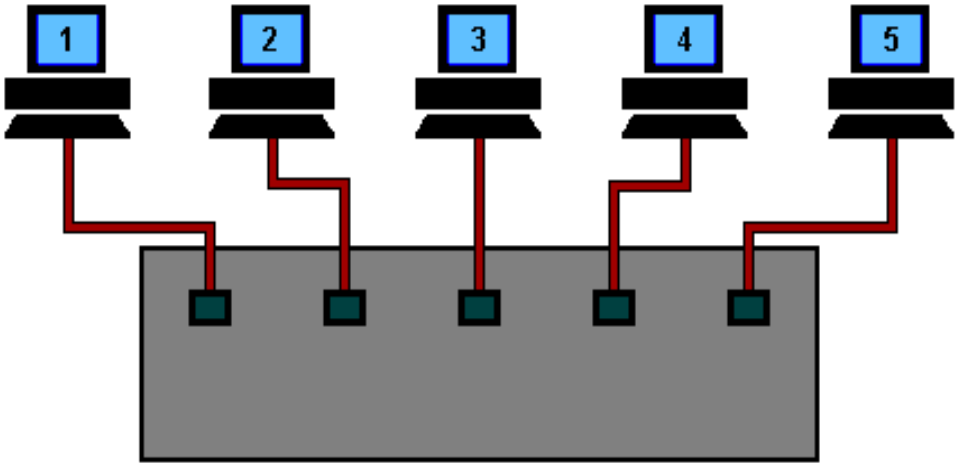
Fast Ethernet 802.3u

Idea: Aumentar la velocidad de Ethernet a 100 Mbps.
Se abandona el cable coaxial y se mantiene el UTP y la FO.

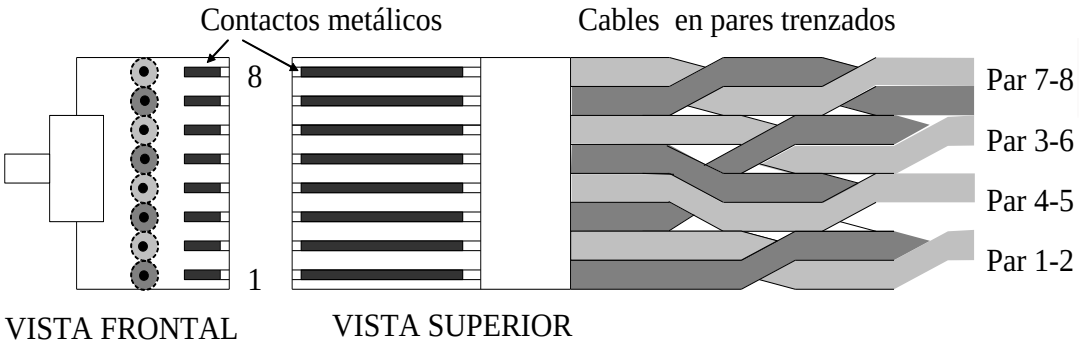
Denominación	Tipo de Cable	Longitud Max.	Transmisión
100-BASE-T4	4 pares UTP-3 o sup.	100 m.	8B6T, NRZ Semi-duplex
100-BASE-TX	2 pares UTP-5 o STP	100 m.	4B5B, NRZI Full-duplex
100-BASE-FX	2 fibras ópticas	2000 m.	4B5B, NRZI Full-duplex

Conmutación (I)

Conmutación (II)



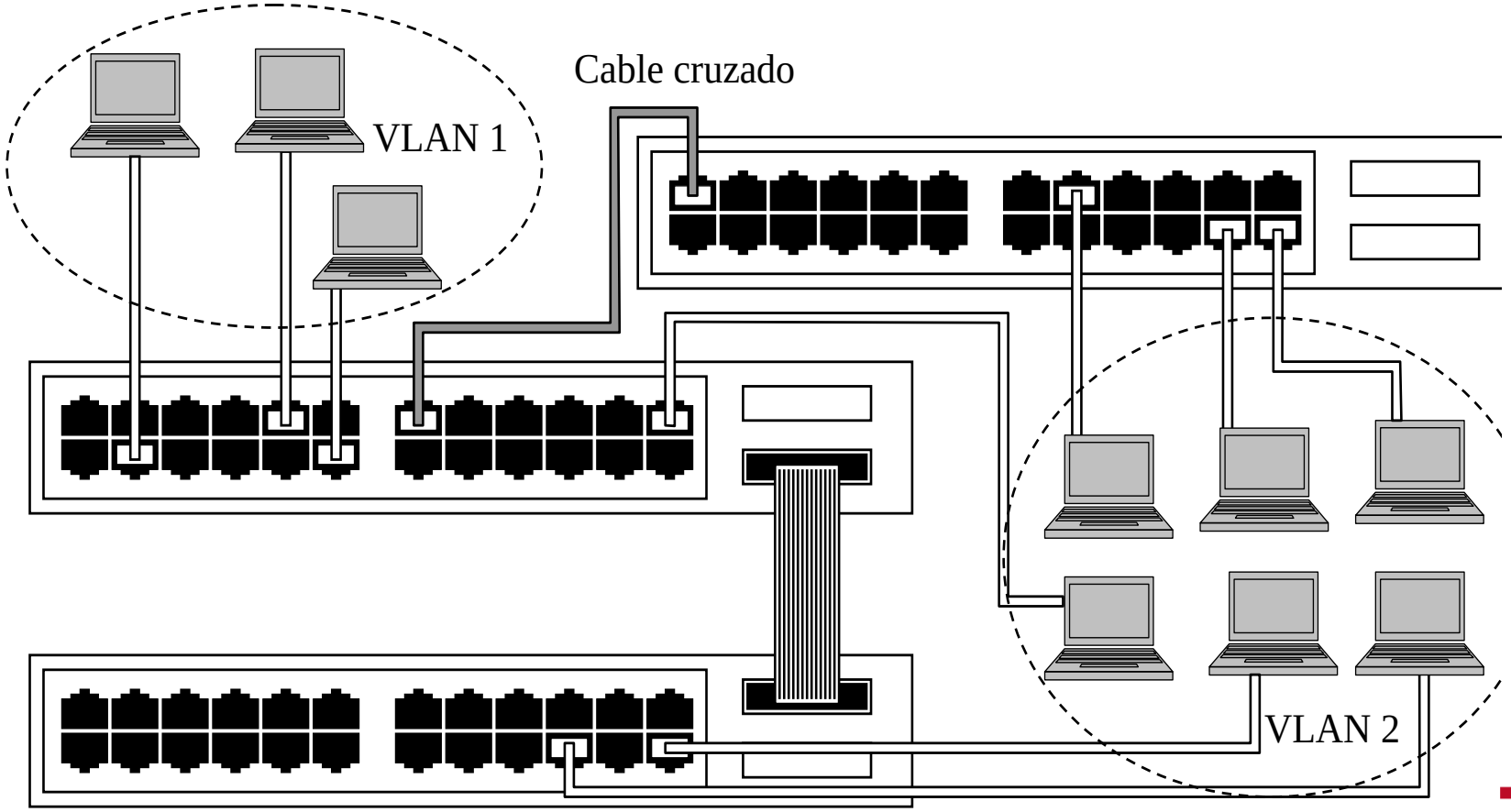
CONECTOR RJ-45



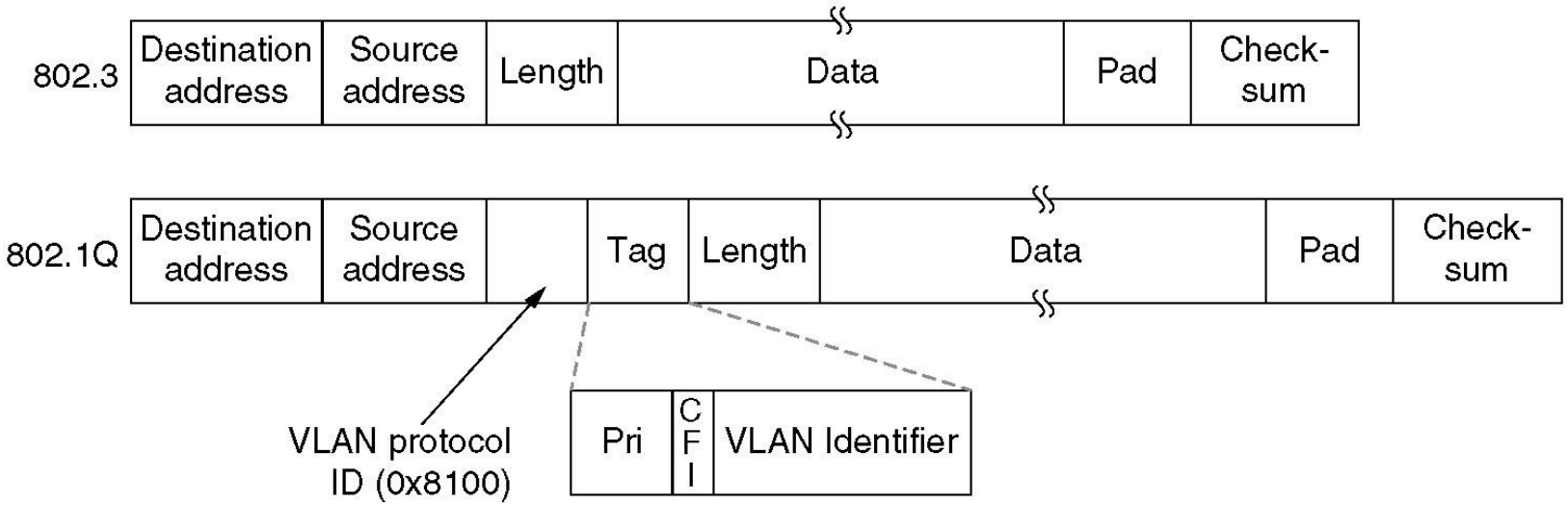
Capacidades de los Conmutadores

- Redes virtuales: VLAN (Etiquetas 802.1Q)
- Agregación de puertos: Port trunks
- Redundancia de conexiones: Spanning tree (802.1D)
- Gestión de la calidad de servicio (Etiquetas 802.1Q).
- Funciones de seguridad:
  - Monitorización de puertos, Estadísticas RMON, Asignación fija de puertos, protección contra tormentas broadcast, etc …

Redes Virtuales (VLAN)

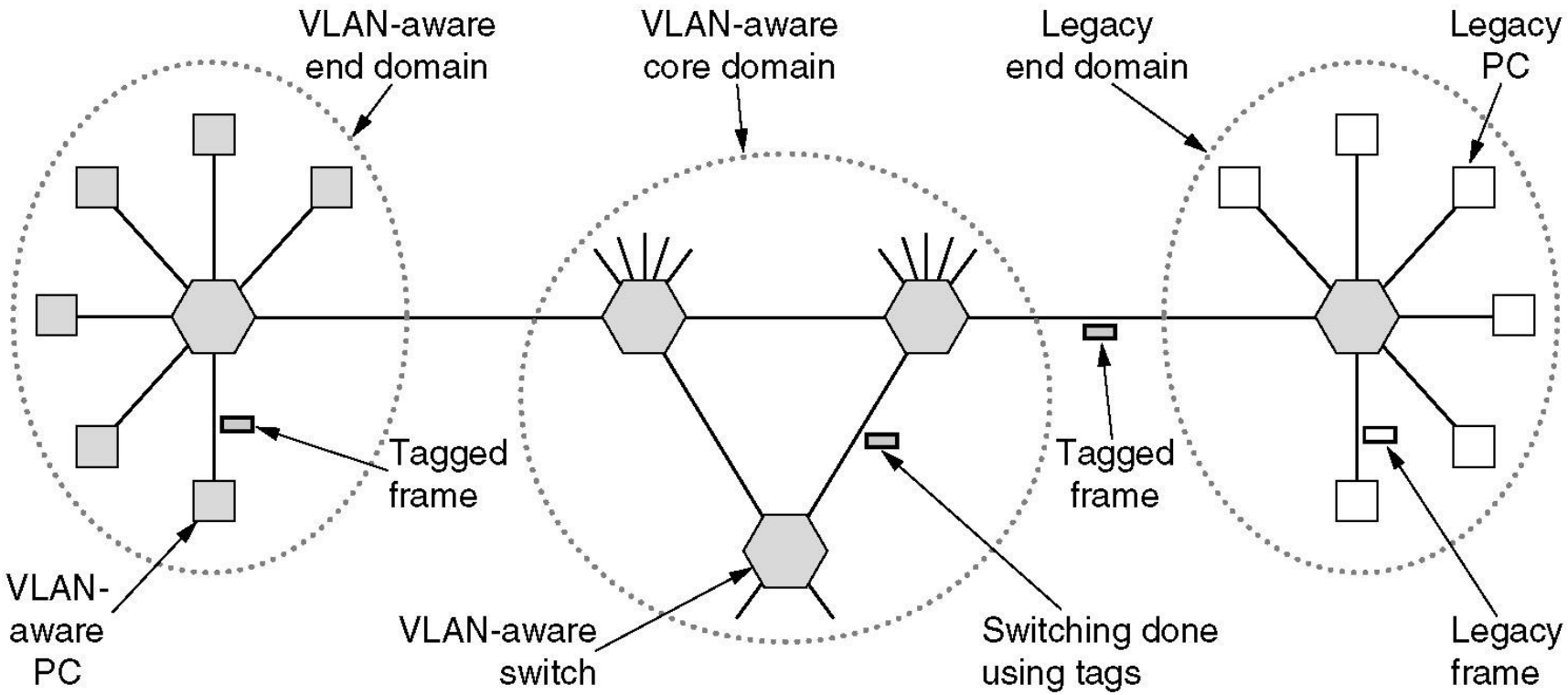


El estándar 802.1Q (I)



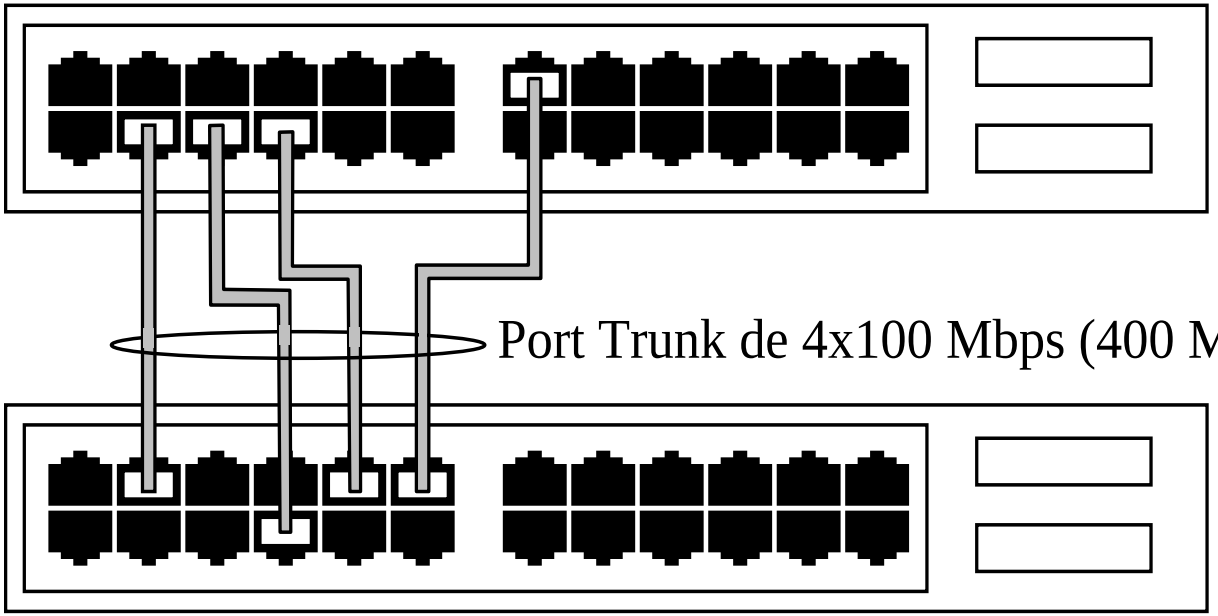
802.3 (*legacy*) y 802.1Q

El estándar 802.1Q (y II)

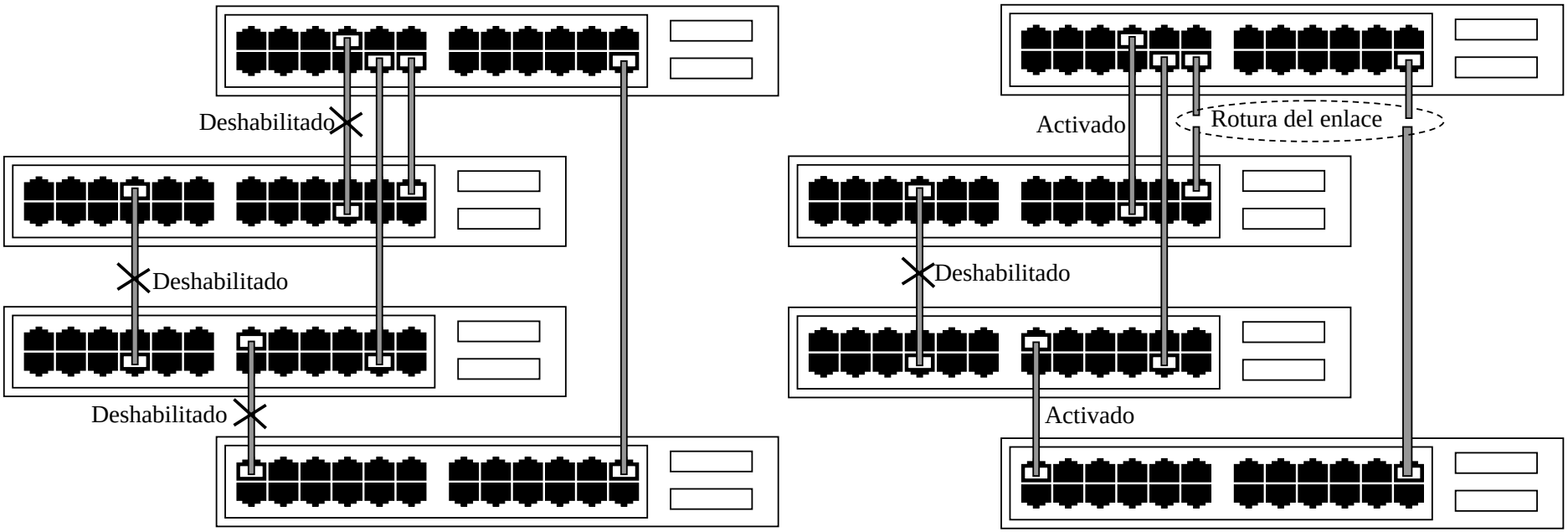


Transición de Ethernet heredada (*legacy)* a Ethernet con soporte VLAN. Los símbolos sombreados soportan VLAN 802.1Q

Agregación de Puertos (*Port Trunks*)



Redundancia de Conexiones



Gigabit Ethernet 802.3z (I)

- **Idea:** Ya puestos estaría bien llegar a 1Gbps…
- En conexiones PC-PC o con conmutación, se abandona CSMA/CD. Funcionamiento dúplex.
- En conexiones con concentradores, puede haber colisiones, por lo que se necesita CSMA/CD:
  - Problemas con los tamaños mínimos de trama. Dos técnicas posibles:
    - Extensión de portadora
    - Ráfagas de trama

Gigabit Ethernet 802.3z (y II)

Name	Cable	Max. segment	Advantages
1000Base-SX	Fiber optics	550 m	Multimode fiber (50, 62.5 microns)
1000Base-LX	Fiber optics	5000 m	Single (10 μ) or multimode (50, 62.5 μ)
1000Base-CX	2 Pairs of STP	25 m	Shielded twisted pair
1000Base-T	4 Pairs of UTP	100 m	Standard category 5 UTP

¡Y ya existe una Ethernet a 10Gbps (802.3ae)!

El IEEE 802.2. Control Lógico del Enlace

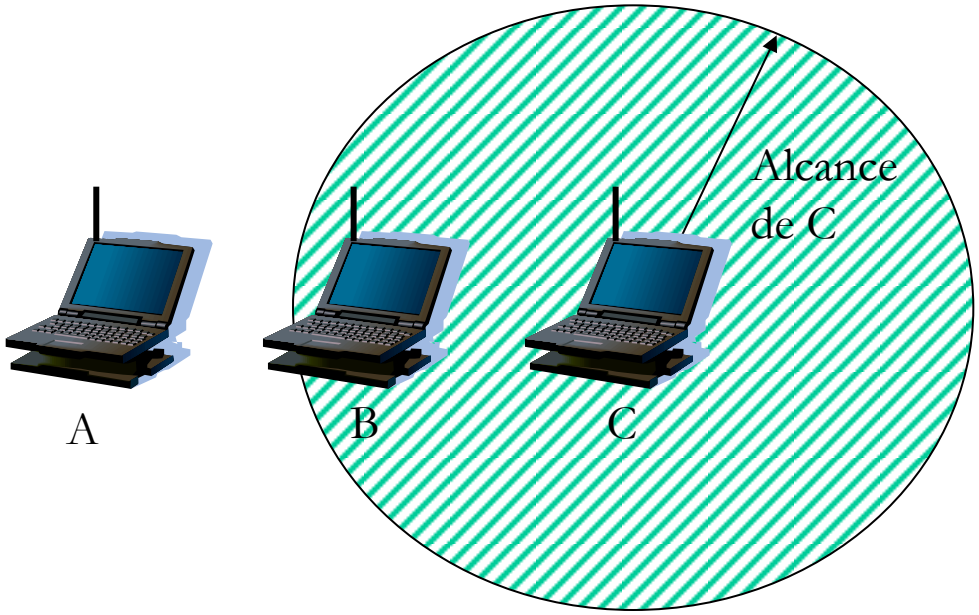
- Estándar que define el LLC, que opera sobre la subcapa MAC para completar la capa de Enlace y uniformizar los distintos estándares de nivel inferior.
- Se añaden puntos de acceso al servicio (DSAP y SSAP) de 8 bit para la multiplexación, sólo asignados a “estándares internacionales” (IP no tiene).
- Además incluye campos para números de secuencia.
- Ofrece tres tipos de servicio:
  - Tipo 1 (sin conexión)
  - Tipo 2 (orientado a la conexión)
  - Tipo 3 (sin conexión, pero con acuse de recibo – sólo para enlaces punto a punto)
- Hay un estándar de Internet para encapsular IP (usando la extensión SNAP - Subnet Access Protocol- de 802.2), pero casi nunca se usa sobre Ethernet. Sí sobre redes Token Ring, FDDI y otras redes 802.
- MacOS lo utiliza para implementar Apple Talk sobre Ethernet.

Capa Física

	Tasas de transmisión máximas	Rango	Modulación	Frecuencia
802.11a	Hasta 54 Mbps	30 m	OFDM (FHSS)	U-NII (5 GHz)
802.11b	Hasta 11 Mbps	30 m	HR-DSSS	ISM (2'4 GHz)
802.11g	Hasta 54 Mbps	30 m	OFDM (FHSS)	ISM (2'4 GHz)
802.11n	Hasta 540 Mbps	50 m	MIMO-OFDM	ISM (2,4 GHZ)

- Pueden funcionar en dos modos:
  - En presencia de una estación base (generalmente conectada a la red cableada).
  - Sin estación base (red ad-hoc)

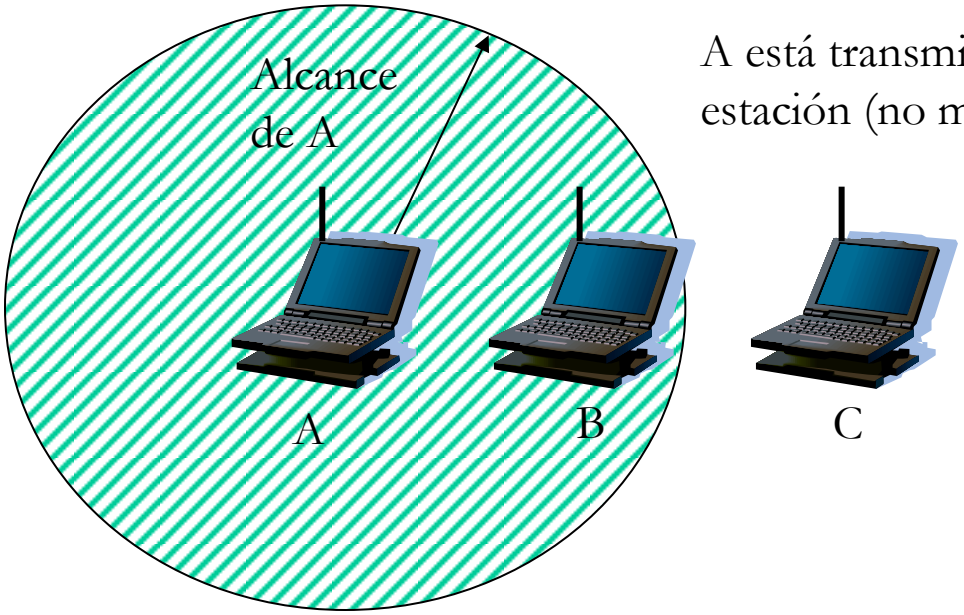
Acceso al Medio: El Problema de la Estación Oculta



C está transmitiendo a B

A quiere transmitir a B: CSMA falla porque no puede detectar que está ocupado

Acceso al Medio: El Problema de la Estación Expuesta



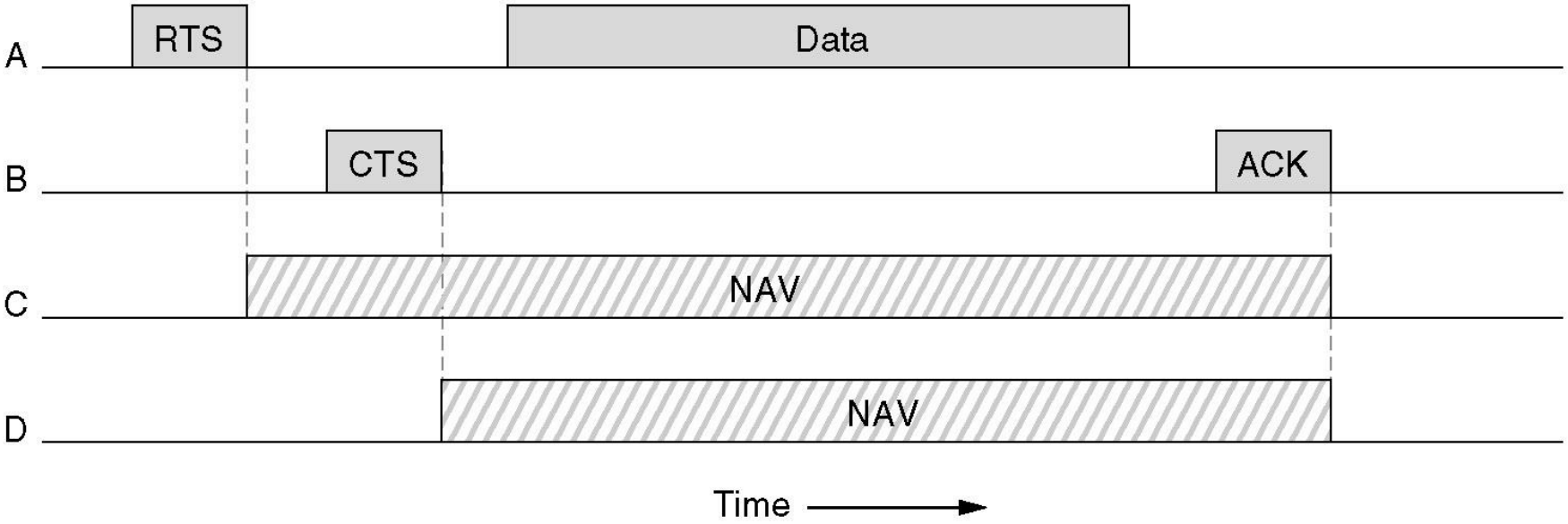
A está transmitiendo a una cuarta estación (no mostrada)

B quiere transmitir a C: CSMA falla porque se detecta la transmisión de A

CSMA/CA

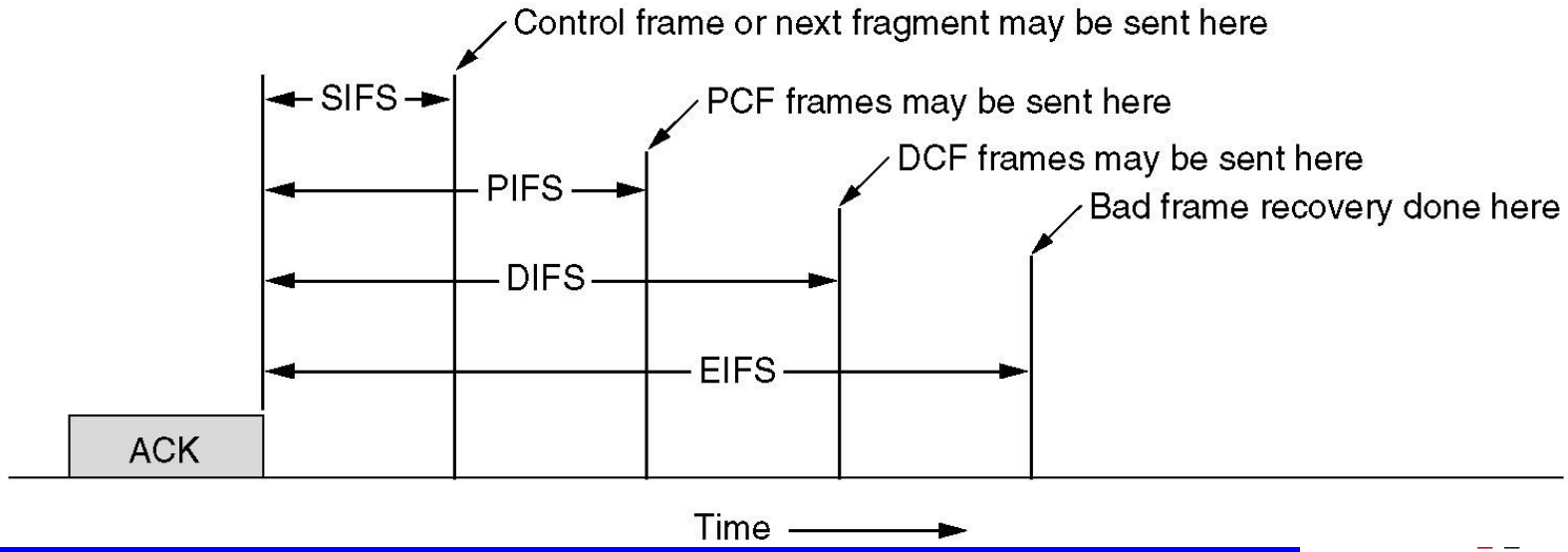
- **Esencia**: Basarse en MACAW y **calcular** el tiempo que el canal estará ocupado. Se denomina **detección del canal virtual.**

Supongamos transmisión entre A y B. C está en el alcance de A. D en el de B pero no en el de A.

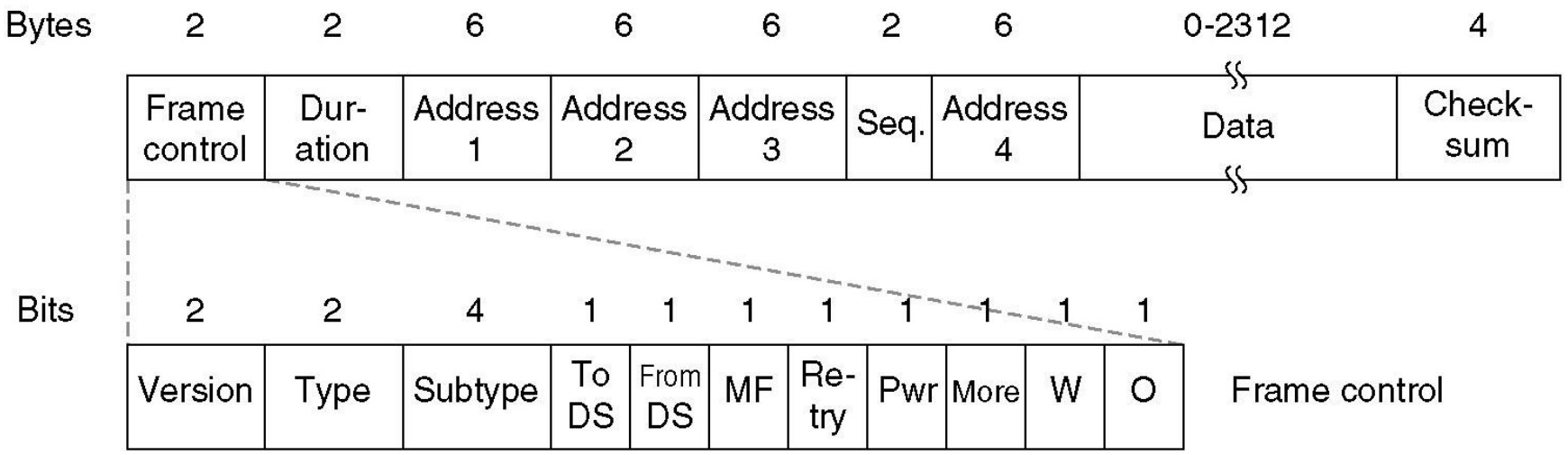


Modos DCF y PCF

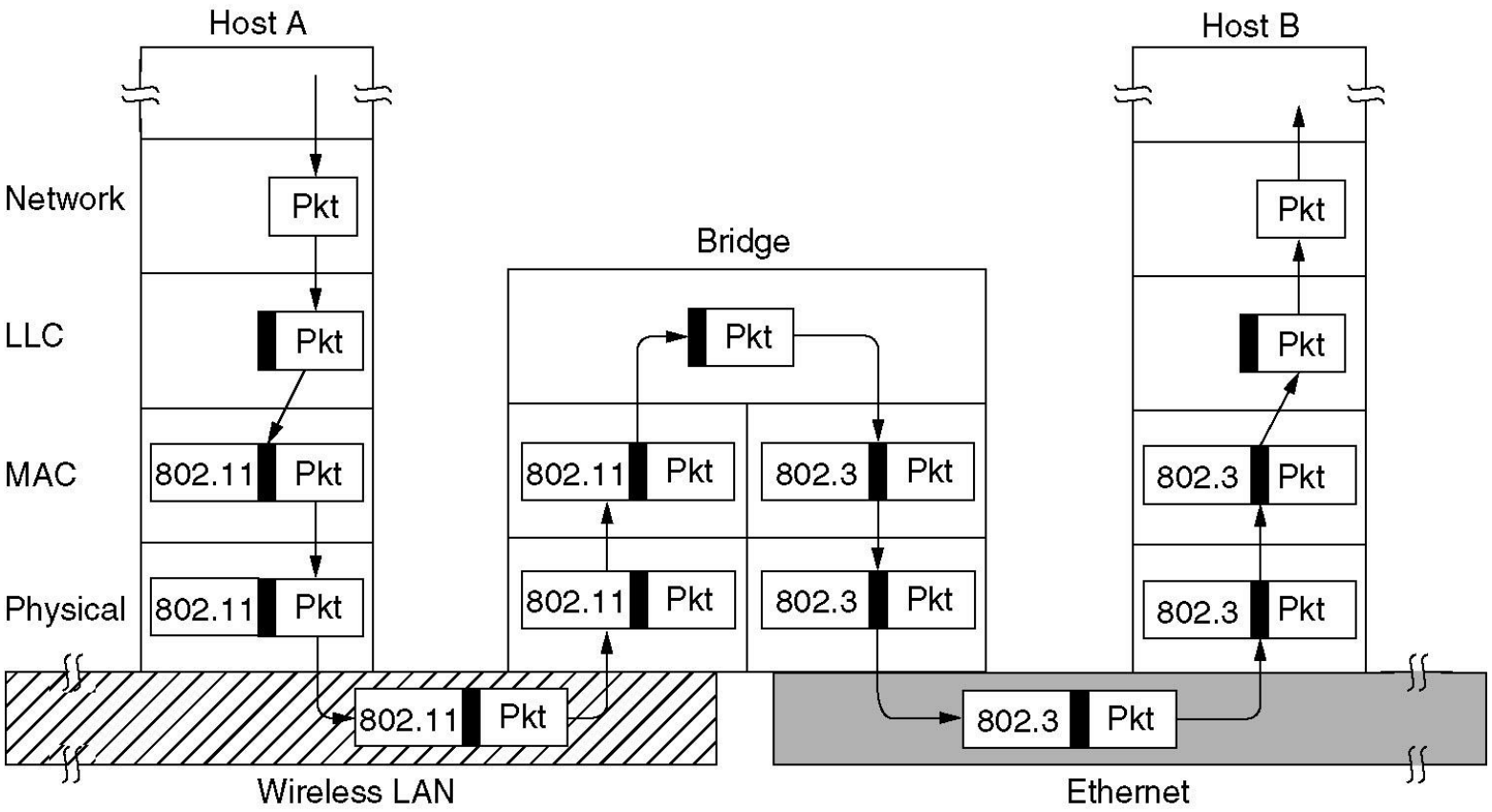
- 802.11 soporta dos modos de funcionamiento:
  - Distribuido (DCF): no hay control central. Se compite por el medio.
  - Puntual (PCF): La estación base sondea los nodos inalámbricos. No hay colisiones.
- Pueden convivir con una cuidada temporización.



Estructura de trama 802.11



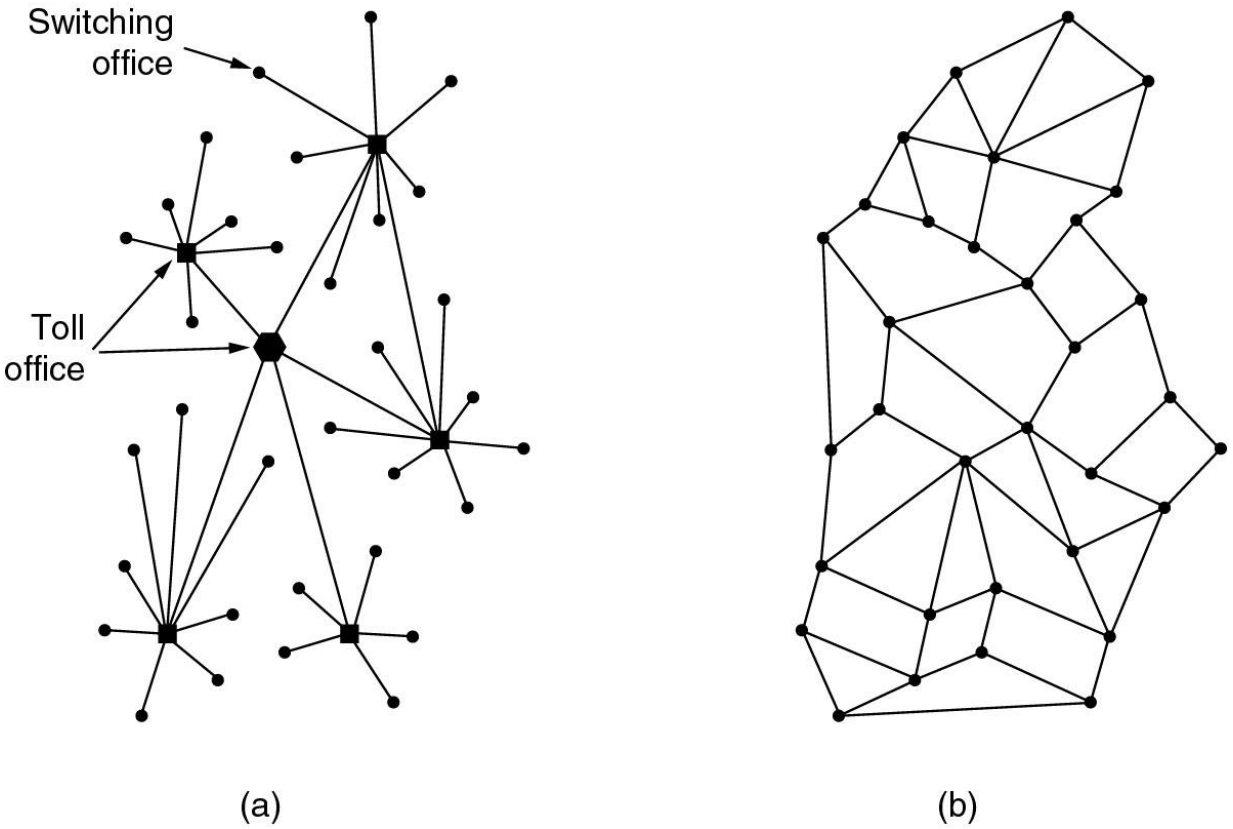
Puentes 802.x a 802.y



Desde ARPANET a Internet (I)

- Octubre1957: La URSS lanza el Sputnik.
- Eisenhower crea ARPA en febrero de 1958.
- Primeros conceptos de comunicaciones: Kleinrock comienza a aplicar la teoría de colas y control de tráfico distribuido en *switches*.
- Comienzo de los 60s: Guerra Fría. Se encarga la creación de una red de comunicaciones indestructible a Paul Baran.
  - Topología de malla.
  - Concepto de redes de paquetes (almacenamiento y reenvío).
- Baran, Kleinrock y Davies crean la red de paquetes, pero AT&T desecha la idea

Desde ARPANET a Internet (II)

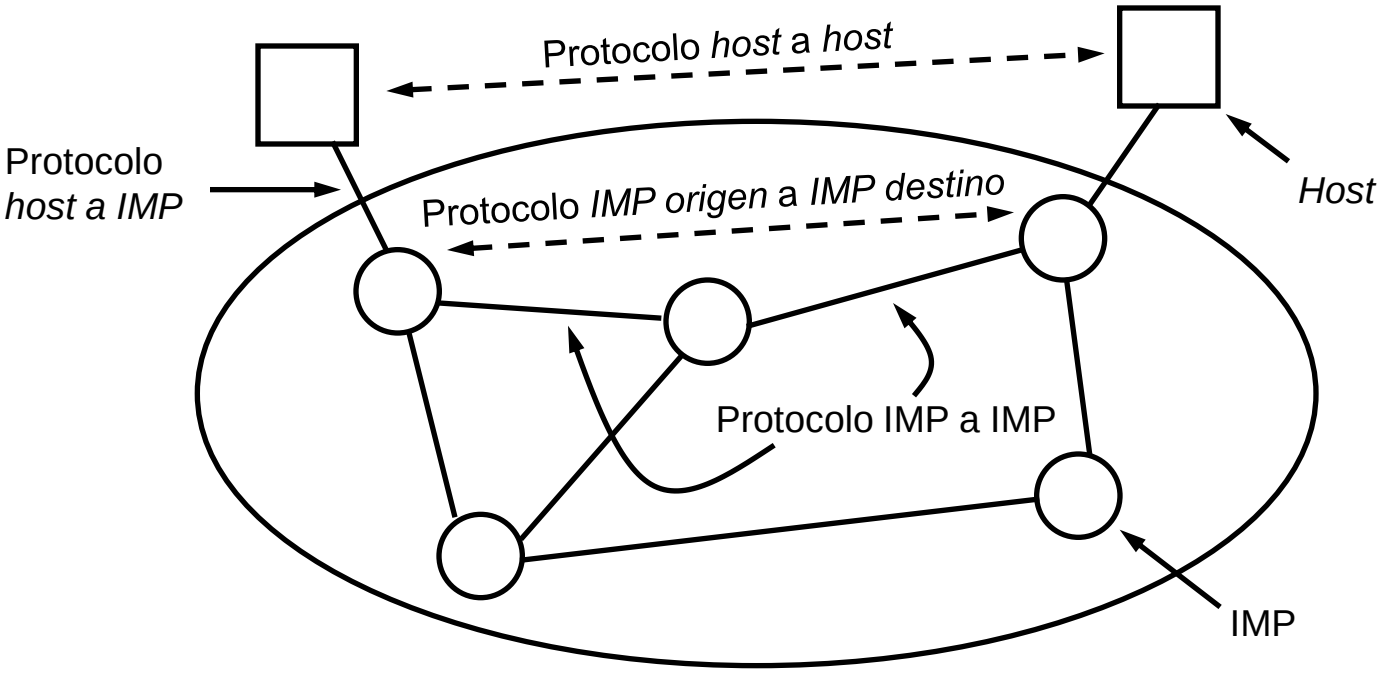


a) Estructura de la red telefónica
b) Estructura propuesta por Paul Baran

Desde ARPANET a Internet (III)

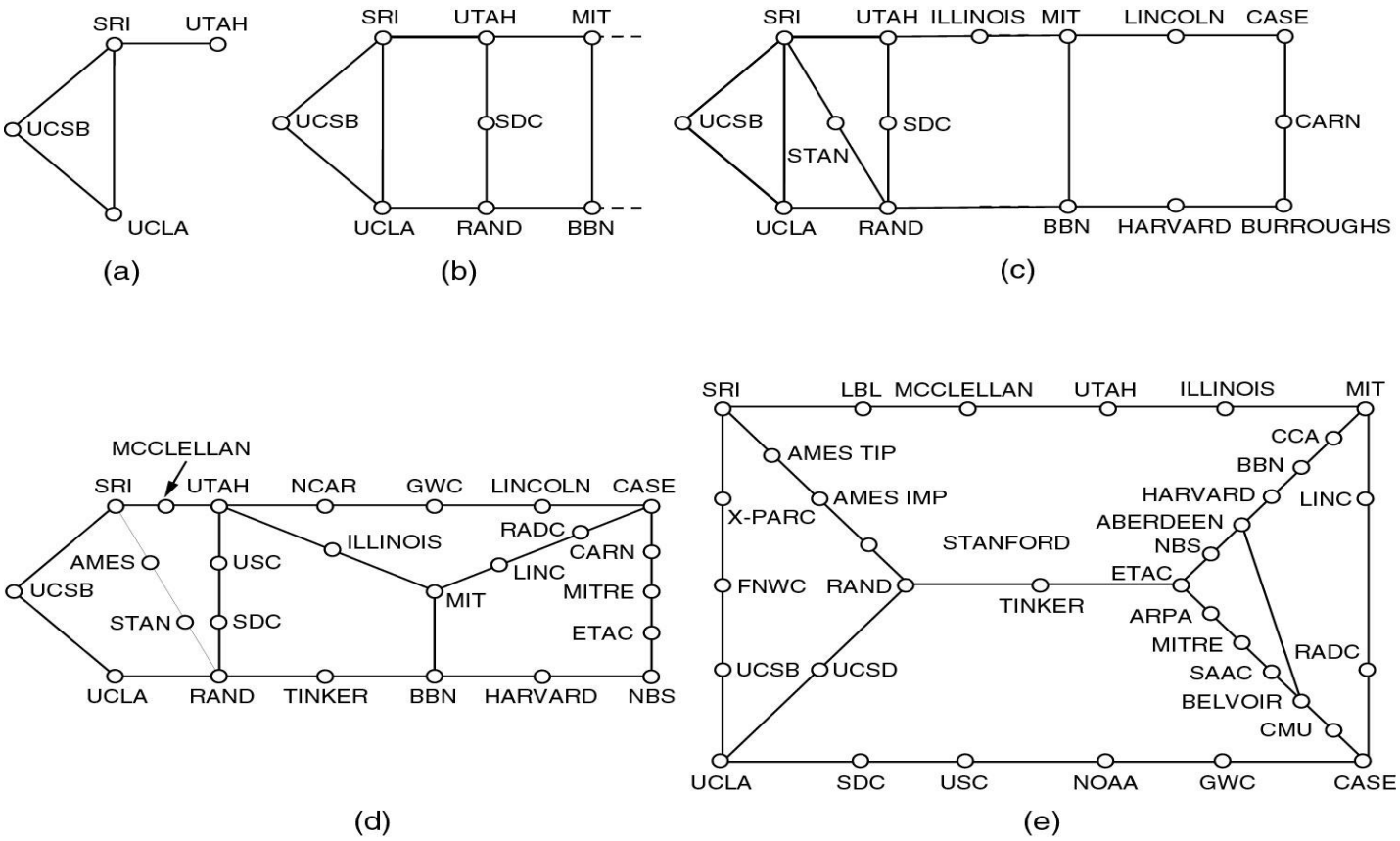
- Años 60. Bob Taylor (ARPA), quien ha trabajado con Licklider, visionario de las redes de computadores, sugiere usar un solo terminal para acceder a todos los computadores. Se trae a Lawrence Roberts para trabajar en el proyecto.
- Se le concede un presupuesto de 1 millón de dólares para construir la primera red experimental.
- 1968 se forma el equipo de trabajo (AT&T e IBM lo rechazan, BBN lo acepta).
- Vinton Cerf, Bob Kahn, estudiantes con Kleinrock, inventan TCP/IP.
- 1969 se conectan los primeros computadores.
- Hasta los años 70 no surgen otras redes, como SNA o Token Ring. Ethernet es incluso posterior.
- La ISO comienza a trabajar en el modelo OSI en 1977

Desde ARPANET a Internet (IV)



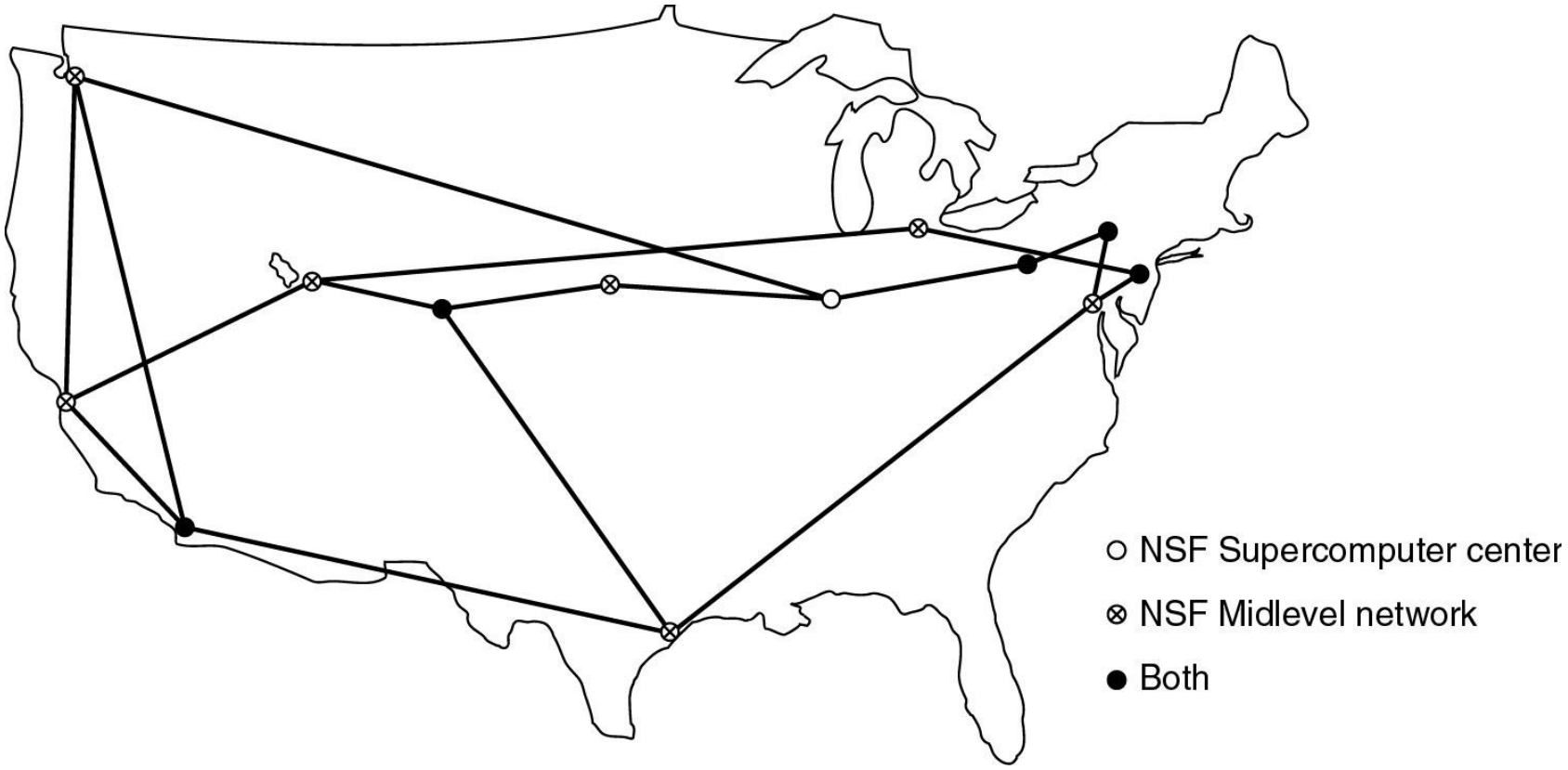
Diseño original de ARPANET

Desde ARPANET a Internet (V)



Crecimiento de ARPANET (a) Diciembre 1969. (b) Julio 1970. (c) Marzo 1971. (d) Abril 1972. (e) Septiembre 1972.

Desde ARPANET a Internet (VI)

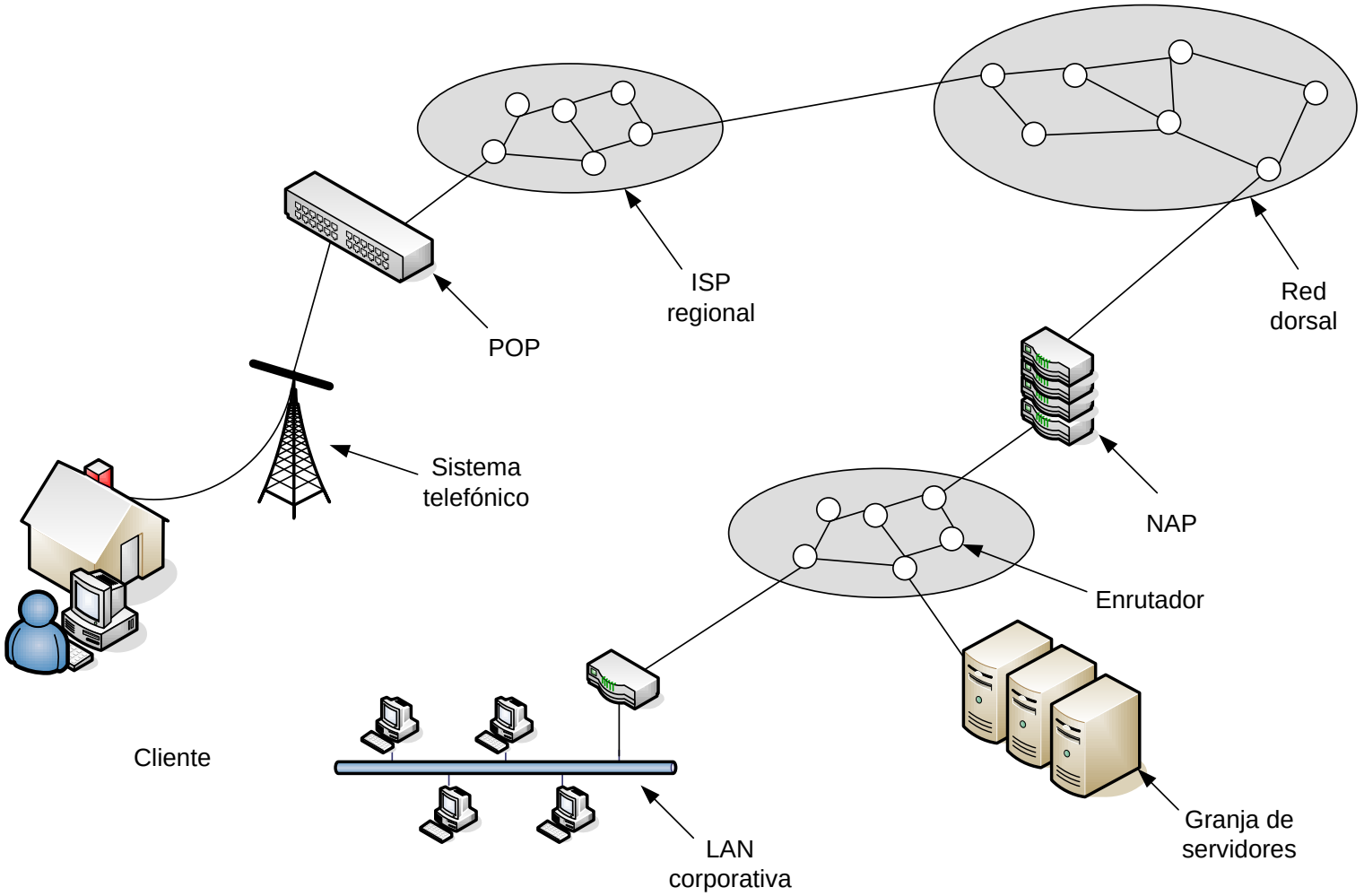


La Red Dorsal NSFNET en 1988

Desde ARPANET a Internet (y VII)

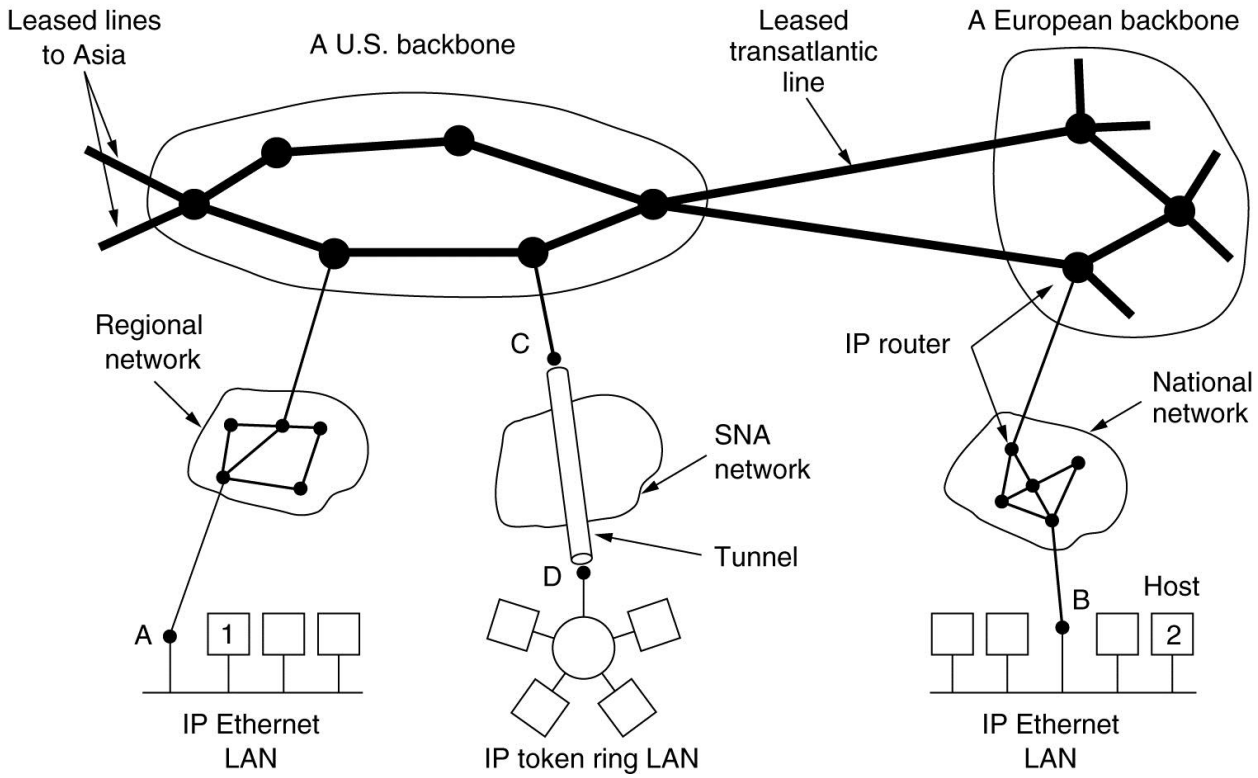
- Las aplicaciones más importantes en la década de los 80 son
  - Terminal remota
  - Transferencia de archivos
  - Correo electrónico
  - Noticias y grupos de discusión
- Existe multitud de información en la red, pero hay que ser un experto para encontrarla (Archie, Gopher,…)
- Principios de los 90: Tim Berners Lee (CERN) inventa la WWW.
- Noviembre 1992. La NSF y el Gobierno de EEUU liberalizan Internet.
- 1993 Mark Andersen desarrolla Mosaic a los 22 años.

Panorama de Internet

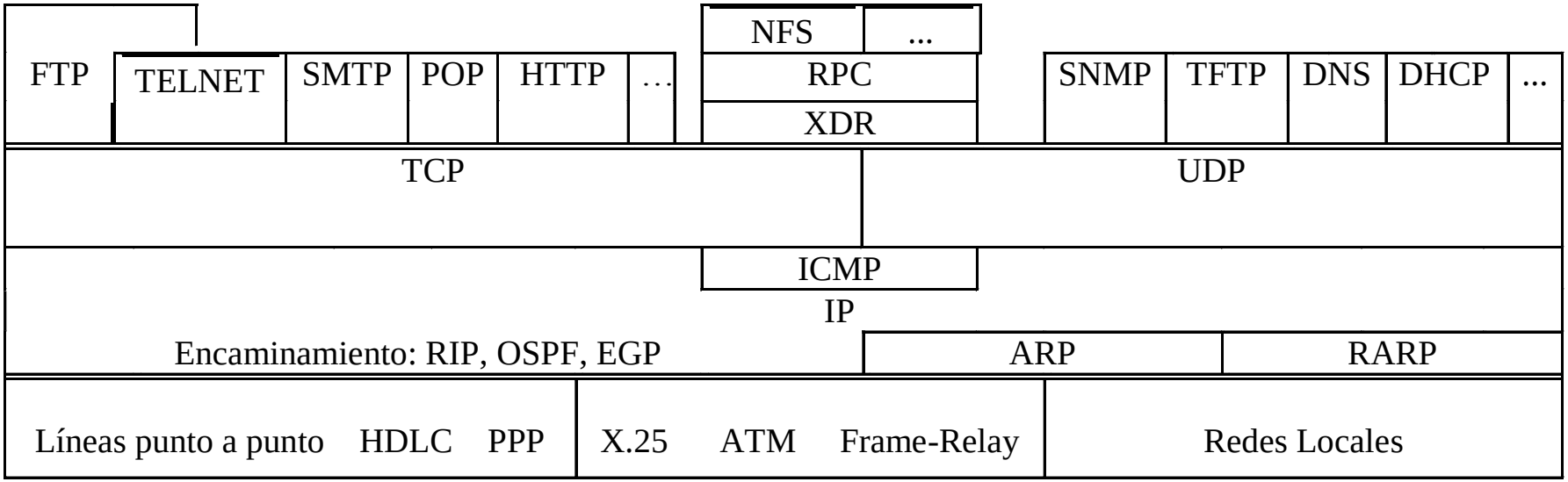


Internet

Se puede ver como un conjunto de **sistemas autónomos (AS)** conectados entre sí por **troncales**.



TCP/IP Una familia de protocolos



Todos los elementos que componen la familia TCP/IP se describen en los RFCs

Principios de diseño de la capa IP

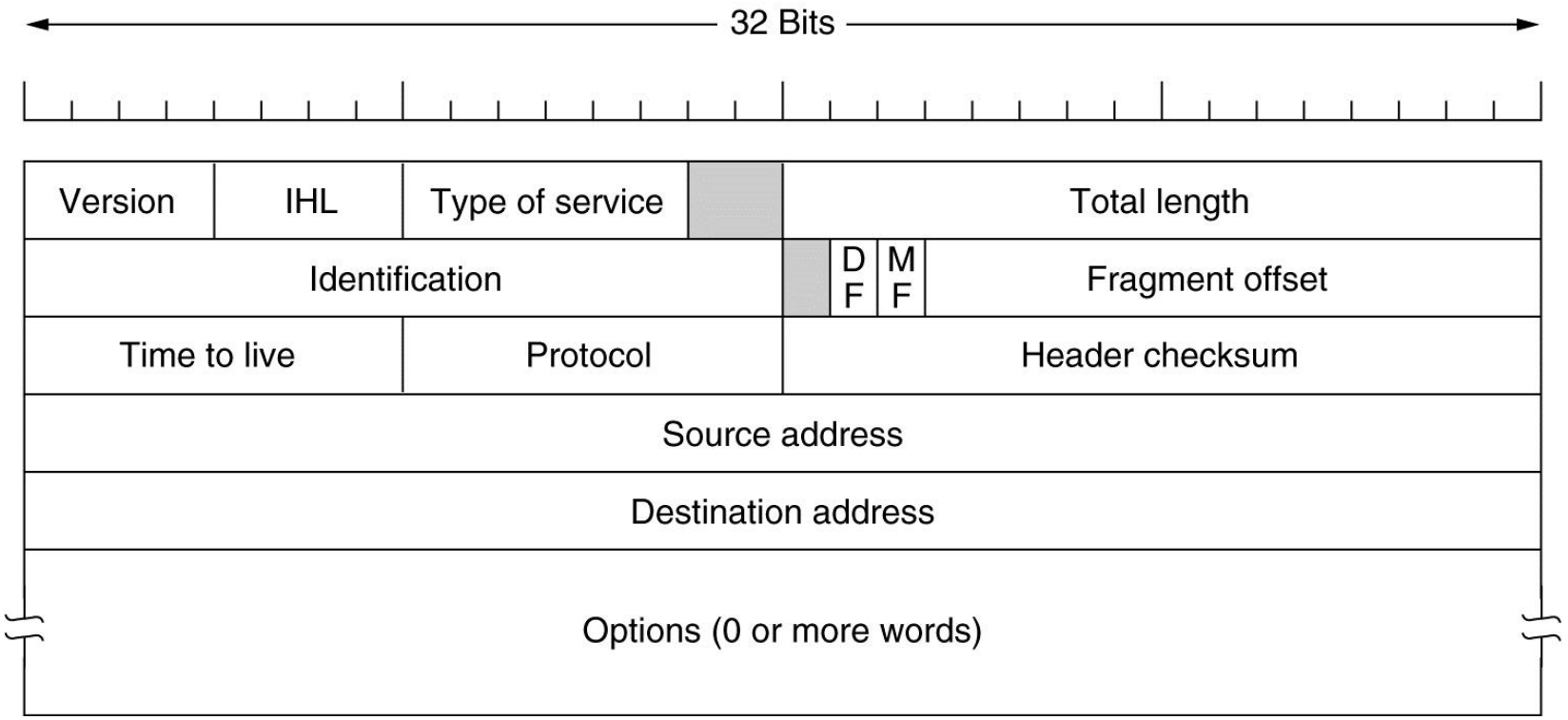
- Se utiliza un protocolo común y único para “aglutinar” todas estas redes y un esquema de direccionamiento global y enfocado a la eficiencia del proceso de encaminamiento.

- Supone un solo tipo de servicio para ofrecer: el de datagrama simple.

- Los principios de diseño se recogen en la RFC 1958 y utiliza las ideas de Clark, 1988 y Saltzser *et al* 1984. En resumen:

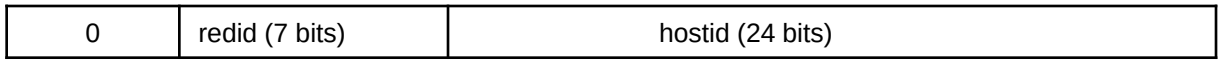
  - Asegúrese de que funciona y que sea simple y modular.
  - Prevea la heterogeneidad
  - Evite parámetros fijos y que los extremos los negocien
  - No es necesario que sea perfecto
  - Sea estricto al enviar y tolerante al recibir
  - Piense en la escalabilidad

El Datagrama IP



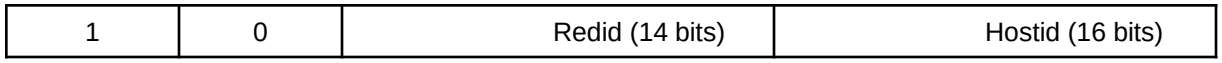
Direcciones IP

Clase A (1.0.0.0 a 126.255.255.255)



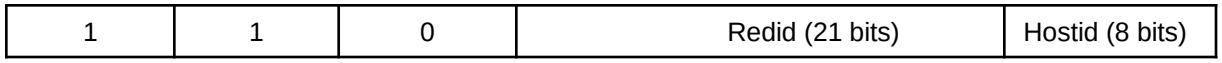
126 redes de 16.777.214 hosts

Clase B (128.0.0.0 a 191.255.255.255)



16.382 redes de 65.534 hosts

Clase C (192.0.0.0 a 223.255.255.255)



2.097.150 redes de 254 hosts

Notas:

Clase D: redes multicast, desde 224.0.0.0 hasta 239.255.255.255 (RFC3171)

Clase E: experimental, desde 240.0.0.0 hasta 254.255.255.255 (RFC 1700)

Direcciones IP reservadas

Algunas direcciones están reservadas (no son asignables a un host):

- hostid=0 significa **este** host, hostid=255 significa **todos** los hosts (difusión)
- redid=0 significa **esta** red (dirección de la red).
- redid=0 y hostid=0 se usa por un host cuando aún no conoce su dirección IP
- 127.x.x.x loopback

Algunas direcciones no se encaminan (no tienen significado global) y se usan en sistemas locales:

- Clase A: direcciones de la 10.0.0.0 a la 10.255.255.255 (una red de clase A)
- Clase B: direcciones de la 172.16.0.0 a la 172.31.255.255 (16 redes de clase B)
- Clase C: direcciones de la 192.168.0.0 a la 192.168.255.255 (256 redes de clase C)

Subredes

- **Problema**: Todos los hosts de la misma red comparten la misma dirección de red. Si una organización quiere diferenciar en distintas redes necesita adquirir varias clases de direcciones que deben ser anunciadas globalmente **(¿por qué?)**.

- **Solución**: Utilizar una sola dirección de red y dividir internamente el *hostid* en **subred** y host.

1	0	Redid (14 bits)	Subred (6 bits)	Hostid (10 bits)

Una dirección de clase B subdividida en 64 subredes de 1024 hosts. La **máscara de subred** es 11111111111111111111110000000000 ó 255.255.252.0

Classless InterDomain Routing (CIDR)

- **Problema**: La asignación de clases es ineficiente. Imaginemos un organismo que necesita unas 1000 direcciones. Si le asignamos una clase B desperdiciamos direcciones, si le asignamos 4 clases C las tablas de los encaminadores necesitan espacio para las 4 (**explosión de las tablas de rutas**).

- **Solución**: Asignar bloques contiguos de clases C y utilizar una máscara para tener sólo una entrada en la tabla de rutas:

192.60.128.0	(11000000.00111100.10000000.00000000)	Dirección de subred de clase C
192.60.129.0	(11000000.00111100.10000001.00000000)	Dirección de subred de clase C
192.60.130.0	(11000000.00111100.10000010.00000000)	Dirección de subred de clase C
192.60.131.0	(11000000.00111100.10000011.00000000)	Dirección de subred de clase C

192.60.128.0	(11000000.00111100.10000000.00000000)	Dirección de la superred
255.255.252.0	(11111111.11111111.11111100.00000000)	Máscara de la superred
192.60.131.255	(11000000.00111100.10000011.11111111)	Dirección broadcast

CIDR – Ejemplo

Sitio	Nº direcciones	Rango	Notación
S1	2048	194.24.0.0 - 194.24.7.255	194.24.0.0/21
S3	1024	194.24.8.0 - 194.24.11.255	194.24.8.0/22
-	1024	194.24.12.0 - 194.24.15.255	194.24.12.0/22
S2	4096	194.24.16.0 - 194.24.31.255	194.24.16.0/20

Cuando llega un datagrama el encaminador intenta averiguar la **dirección base** de la red utilizando las máscaras:

- **194.24.17.4 AND 255.255.248.0 ≠ 194.24.0.0** **NO**
- **194.24.17.4 AND 255.255.240.0 = 194.24.16.0** **SI**
- **194.24.17.4 AND 255.255.252.0 ≠ 194.24.8.0** **NO**

CIDR – Agregación

- **Nota:** En principio todos los encaminadores del mundo deberían almacenar todas las parejas dirección/máscara para poder encaminar el tráfico.
- **Observación:** Muchos encaminadores enviarán los paquetes de las tres redes a través del mismo camino si los sitios S1, S2 y S3 se encuentran en la misma zona geográfica. Si hay (al menos) 3 redes en ese caso, se puede crear la **entrada agregada** 194.24.0.0/19 para todo ese tráfico.
- Por ello se divide parte del espacio de direcciones de clase C en zonas (RFC 1466)
  - Multi-regional 192.0.0.0 - 193.255.255.255
  - Europa 194.0.0.0 - 195.255.255.255
  - Otros 196.0.0.0 - 197.255.255.255
  - Norte América 198.0.0.0 - 199.255.255.255
  - América Central/Sur 200.0.0.0 - 201.255.255.255
  - Asia/Pacifico 202.0.0.0 - 203.255.255.255
  - Otros 204.0.0.0 - 207.255.255.255
- Además se asignan bloques sólo a ISPs grandes quienes los asignan a su vez a ISPs más pequeños hasta el usuario final.

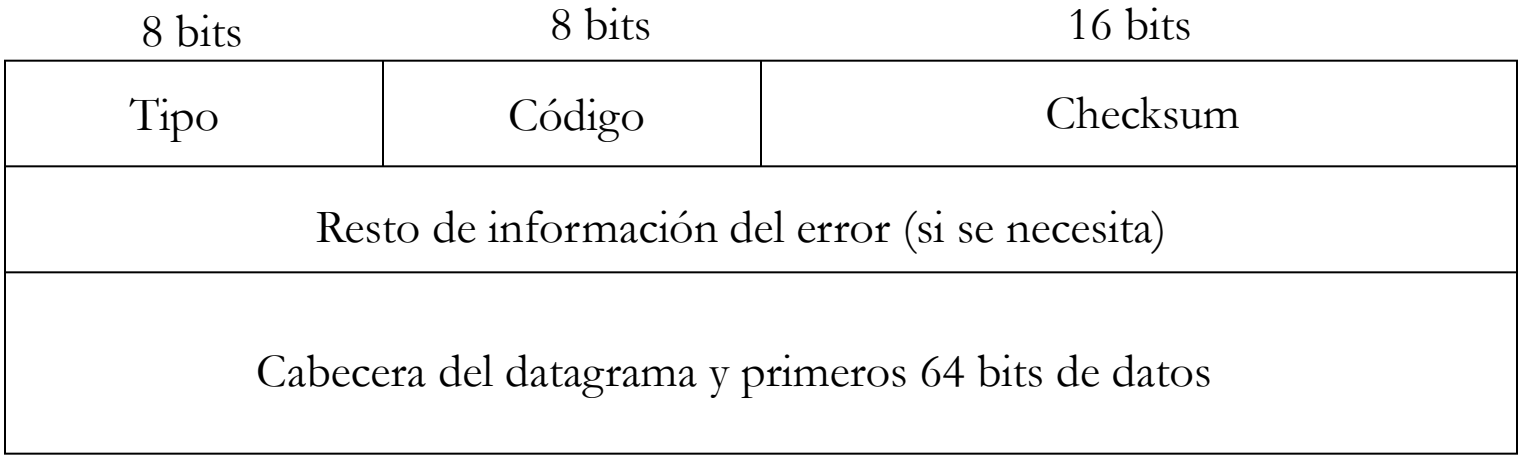
Encaminamiento en IP

- Distinguir entre enrutamiento *dentro* del AS y *entre* ASs:
  - Dentro de un AS el objetivo es llevar paquetes de origen a destino de manera óptima: **IGP** (OSPF, IS-IS, RIP,…)
  - Entre ASs se debe lidiar con temas políticos, como no atravesar determinados ASs en una ruta o no aceptar paquetes “extranjeros” en un AS determinado: **EGP** (BGP)

Protocolo de Mensajes de Control en Internet: ICMP (RFC 792)

- **Idea básica**: Tener un mecanismo que permita informar de errores ocurridos en el tránsito de un paquete.
  - Distinguir diferentes tipos de mensajes: destino inalcanzable, tiempo de vida excedido, etc.
  - Los mensajes se especifican, además, con un código. Ejemplo: un destino puede ser inalcanzable (mensaje 3) porque el paquete no se puede fragmentar (código 4).
  - Además se incluye la cabecera IP del datagrama que causó el error y los primeros 64 bits de datos.
- Los mensajes ICMP se envían dentro de datagramas IP, aunque se procesan de manera distinta por los encaminadores.
  - No se generan en respuestas a datagramas conteniendo mensajes ICMP
  - No se generan más que para el primer fragmento del datagrama
  - No se generan para datagramas con direcciones multicast o especiales
- **Pregunta**: ¿Cómo podemos *reconocer* mensajes ICMP encapsulados en datagramas IP?

ICMP – Formato del mensaje



Campo TIPO	Tipo de mensaje ICMP	Campo TIPO	Tipo de mensaje ICMP
0	Respuesta de eco	12	Problema de parámetro
3	Destino inalcanzable	13	Petición de grabar tiempos
4	Disminución de flujo de la fuente	14	Respuesta de grabar tiempos
5	Redireccionar (cambiar la ruta)	17	Petición de máscara de direcciones
8	Petición de eco	18	Respuesta de máscara de direcciones
11	Tiempo excedido por el datagrama		

ICMP – *ping*

- *ping* es una herramienta que hace uso del protocolo ICMP (mensajes ECHO REQUEST y ECHO REPLY) para comprobar la conectividad de una máquina en Internet.

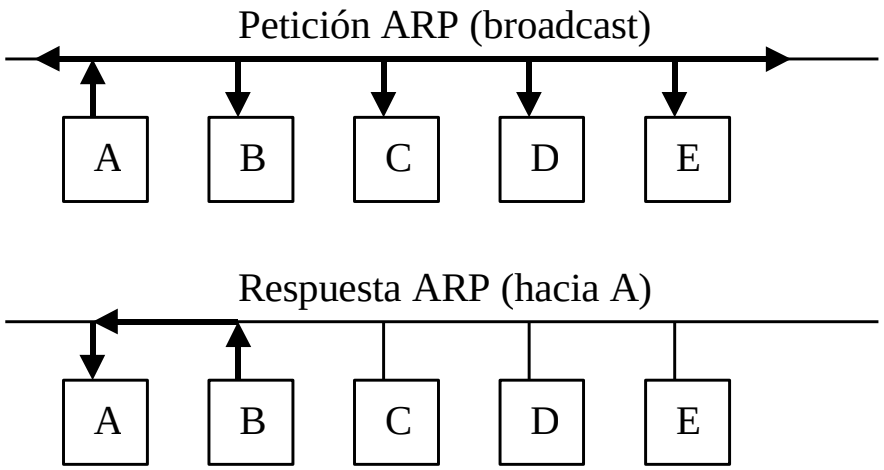
```
>ping www.swcombine.com

Haciendo ping a www.swcombine.com [72.21.61.150] con 32 bytes de datos:

Respuesta desde 72.21.61.150: bytes=32 tiempo=200ms TTL=47
Tiempo de espera agotado para esta solicitud.
Respuesta desde 72.21.61.150: bytes=32 tiempo=185ms TTL=47
Respuesta desde 72.21.61.150: bytes=32 tiempo=166ms TTL=47

Estadísticas de ping para 72.21.61.150:
    Paquetes: enviados = 4, recibidos = 3, perdidos = 1
    (25% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 166ms, Máximo = 200ms, Media = 183ms
```

ICMP – *traceroute*

- *traceroute* envía segmentos UDP y utiliza los mensajes ICMP "tiempo excedido" y "puerto inaccesible" para encontrar la ruta seguida hasta un destino.

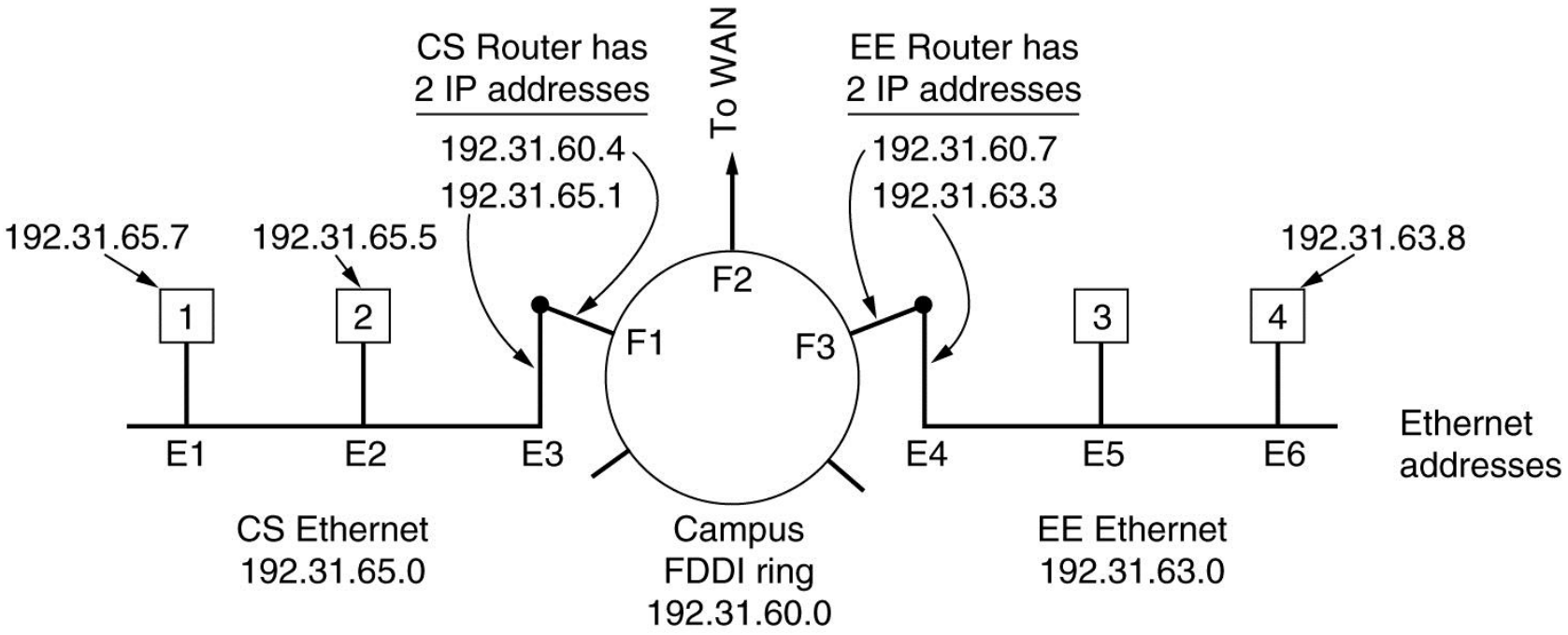
```
traceroute to hecate.edv.uniovi.es (156.35.152.5), 30 hops max, 38 byte packets
 1  POD-C-VL4.GW.CMU.NET (128.2.4.1)  0.223 ms  0.172 ms  0.166 ms
 2  CORE0-POD-C-CYH.GW.CMU.NET (128.2.0.186)  0.194 ms  0.170 ms  0.167 ms
 3  POD-I-CYH-VL940.GW.CMU.NET (128.2.0.205)  0.198 ms  0.184 ms  0.184 ms
 4  bar-cmu-ge-4-0-0-2.3rox.net (192.88.115.185)  0.267 ms  0.292 ms  0.266 ms
 5  leviathan-bar-te0-0-0-1-508.3rox.net (192.88.115.85)  1.318 ms  0.825 ms  0.797 ms
 6  wash-psc10G.layer3.nlr.net (192.88.115.165)  7.980 ms  6.171 ms  5.928 ms
 7  newy-wash-98.layer3.nlr.net (216.24.186.22)  11.767 ms  11.512 ms  11.487 ms
 8  216.24.184.86 (216.24.184.86)  12.658 ms  12.558 ms  12.567 ms
 9  so-7-0-0.rt1.ams.nl.geant2.net (62.40.112.133)  95.897 ms  95.875 ms  95.902 ms
10  so-6-2-0.rt1.fra.de.geant2.net (62.40.112.57)  101.700 ms  101.721 ms  101.677 ms
11  so-6-2-0.rt1.gen.ch.geant2.net (62.40.112.21)  109.839 ms  109.778 ms  109.837 ms
12  so-7-0-0.rt1.mad.es.geant2.net (62.40.112.26)  131.923 ms  131.919 ms  131.894 ms
13  rediris-gw.rt1.mad.es.geant2.net (62.40.124.54)  131.910 ms  131.882 ms  131.907 ms
14  SO1-1-0.EB-IRIS2.red.rediris.es (130.206.240.1)  131.944 ms  132.232 ms  132.017 ms
15  NAC.AS0-0.EB-Santiago0.red.rediris.es (130.206.250.74)  140.259 ms  140.442 ms  148.814 ms
16  AST.S01-0-0.EB-Santiago0.red.rediris.es (130.206.250.98)  148.289 ms  148.185 ms  148.264 ms
17  uniovi-router.red.rediris.es (130.206.196.42)  151.060 ms  172.058 ms  154.634 ms
...
```

Resolución de Direcciones: ARP (RFC 826)



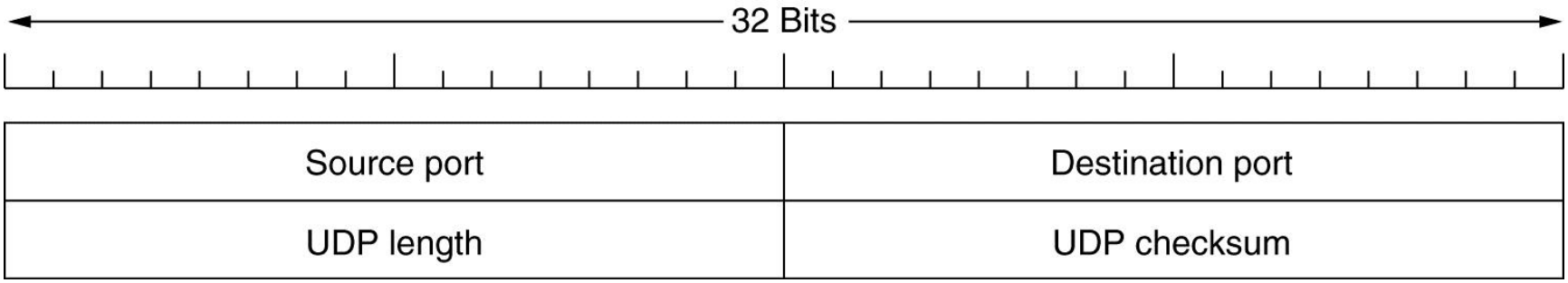
HARDWARE		PROTOCOLO
HLON	PLON	OPERACIÓN
DF ORIGEN (octetos 0-3)		
DF ORIGEN (octetos 4-5)		DL ORIGEN (octetos 0-1)
DL ORIGEN (octetos 2-3)		DF DESTINO (octetos 0-1)
DF DESTINO (octetos 2-5)		
DL DESTINO (octetos 0-4)		

ARP: ¿Y si el destino no está en la misma LAN?

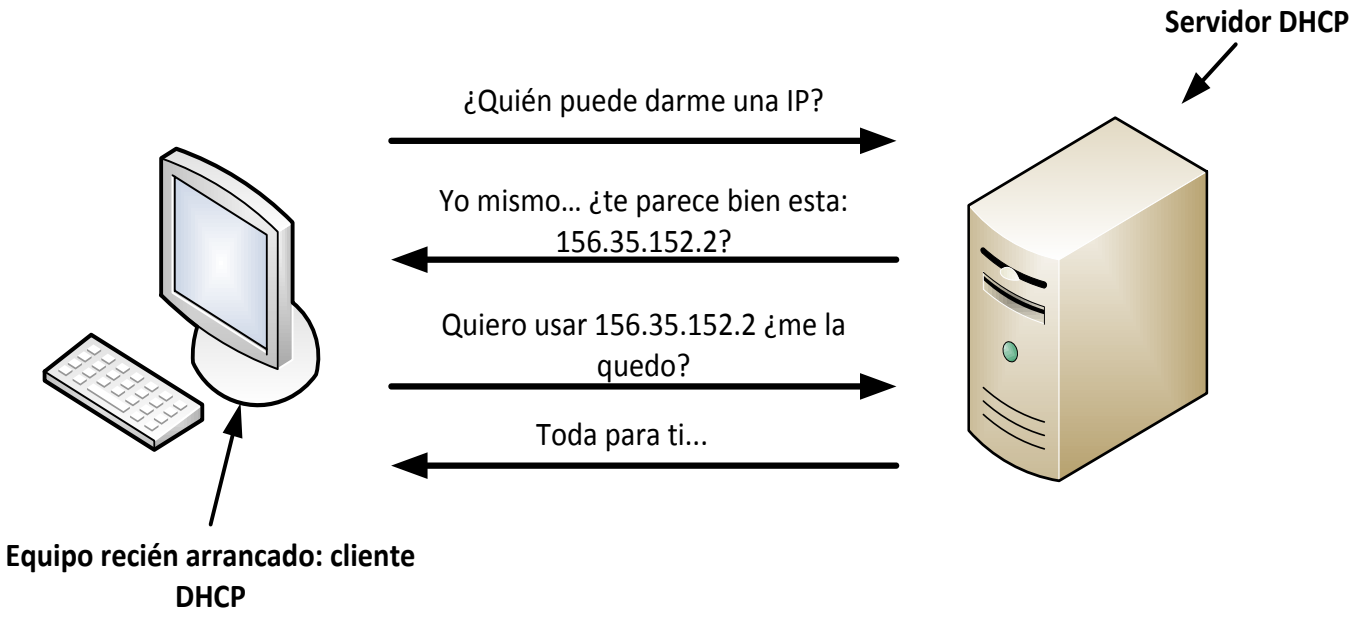


User Datagram Protocol: UDP – RFC 768

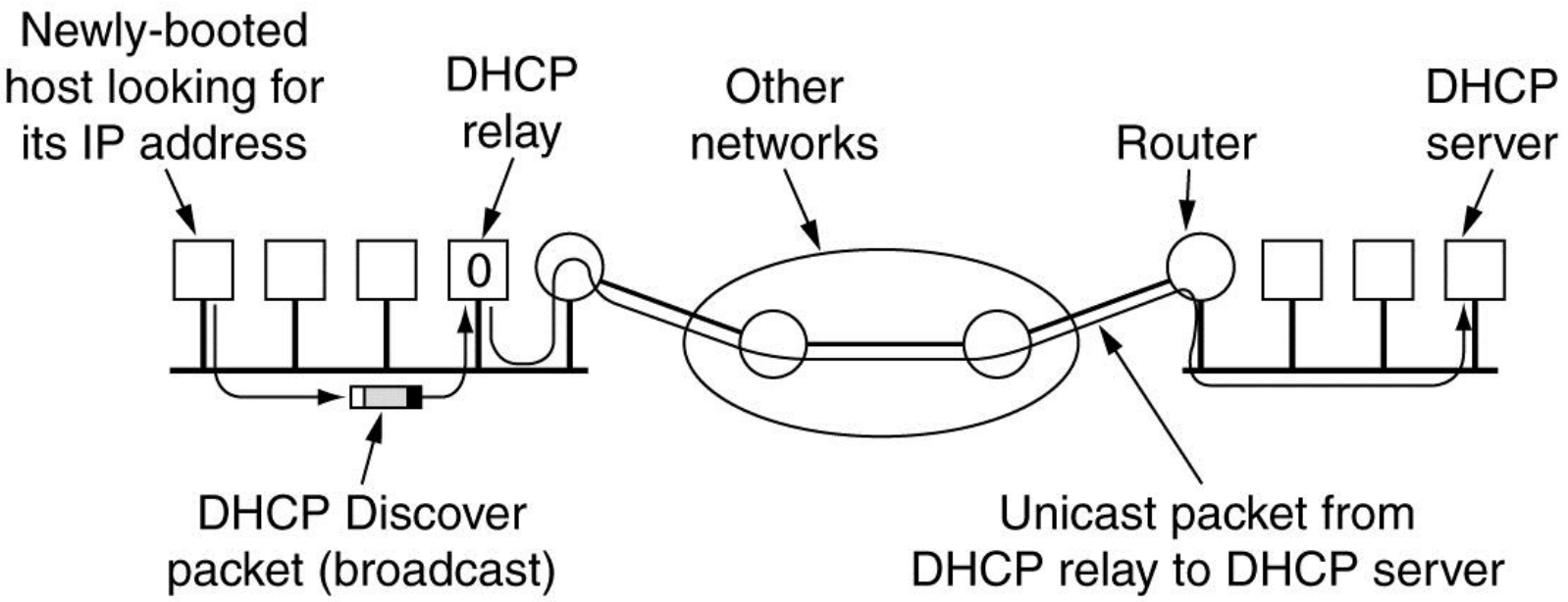
Servicio de Datagrama simple



DHCP (*Dynamic Host Configuration Protocol)*

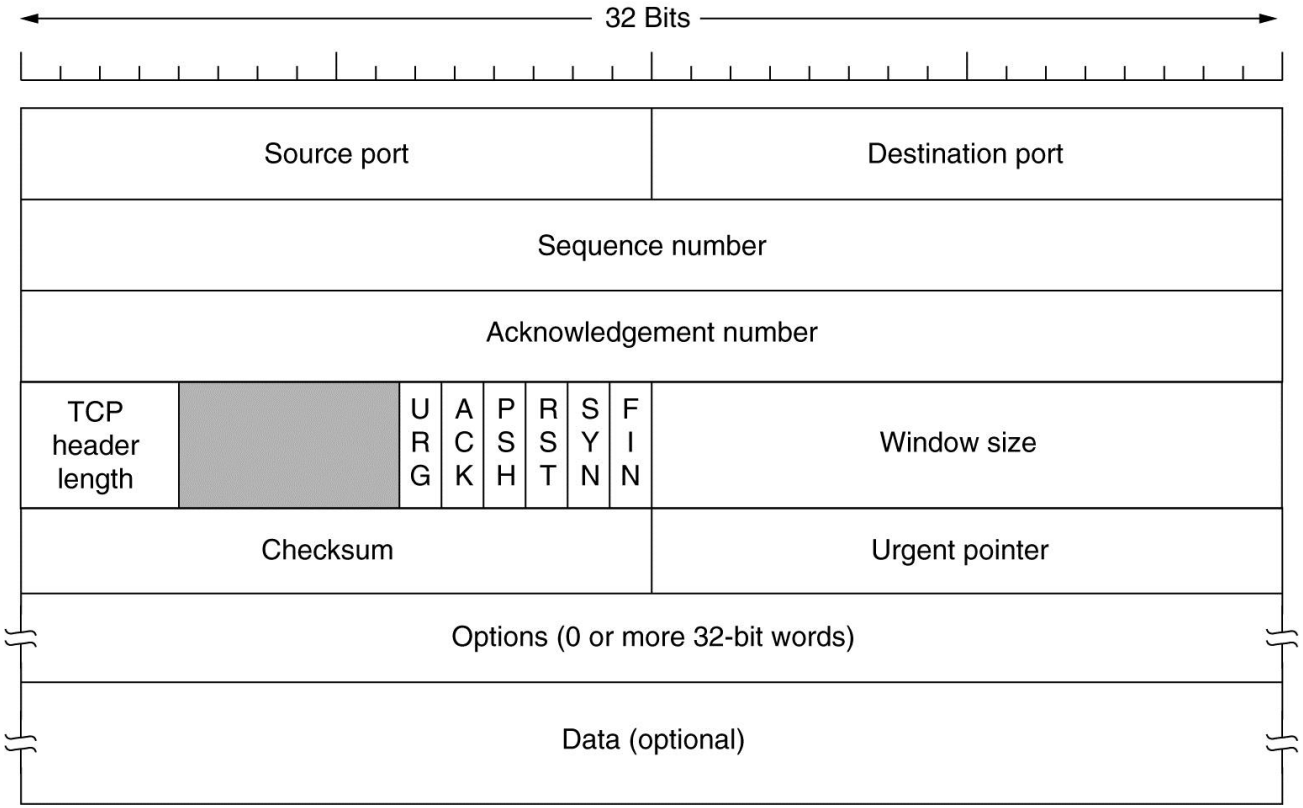


DHCP (*Dynamic Host Configuration Protocol)*

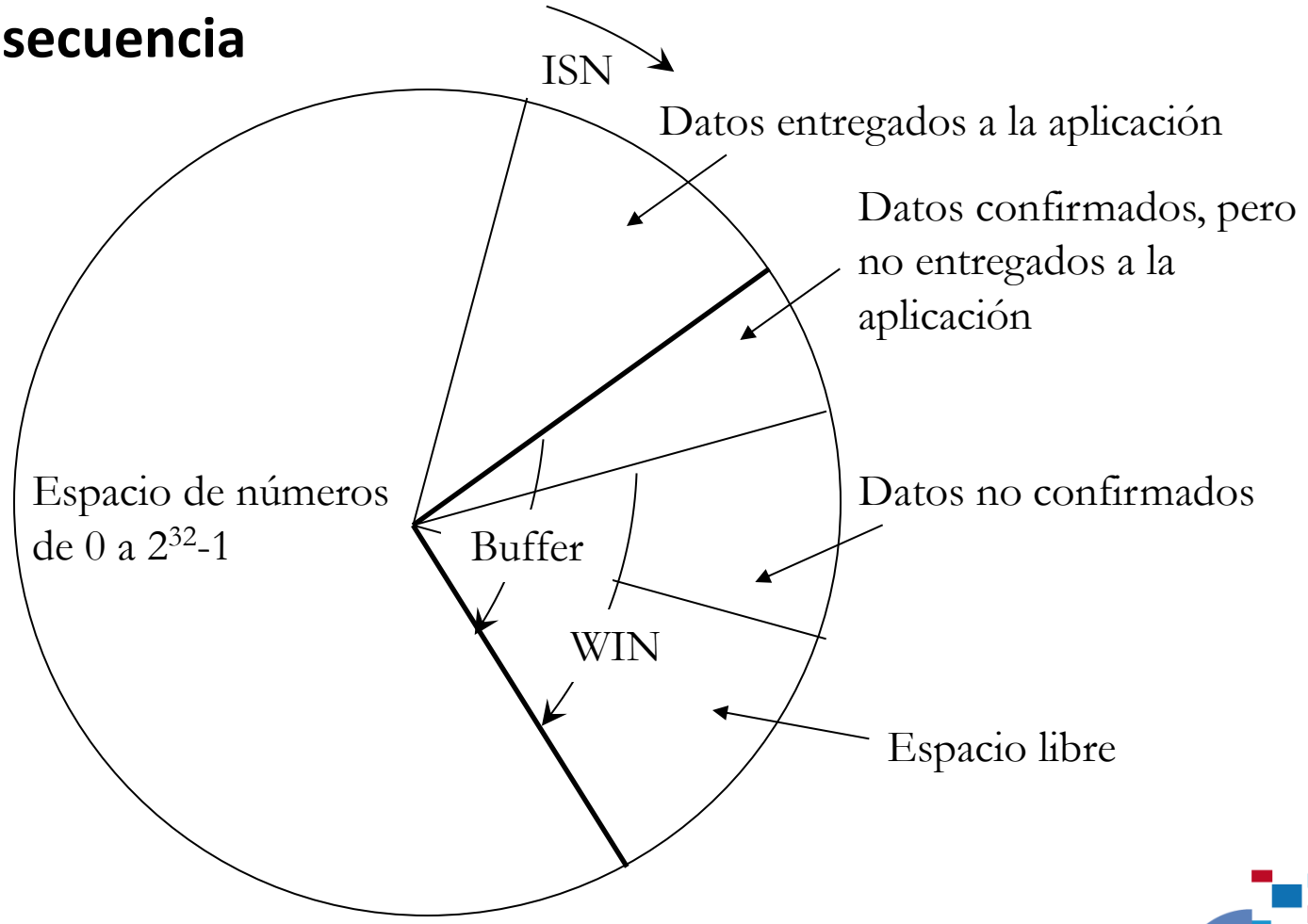


Transmission Control Protocol: TCP – RFC 793

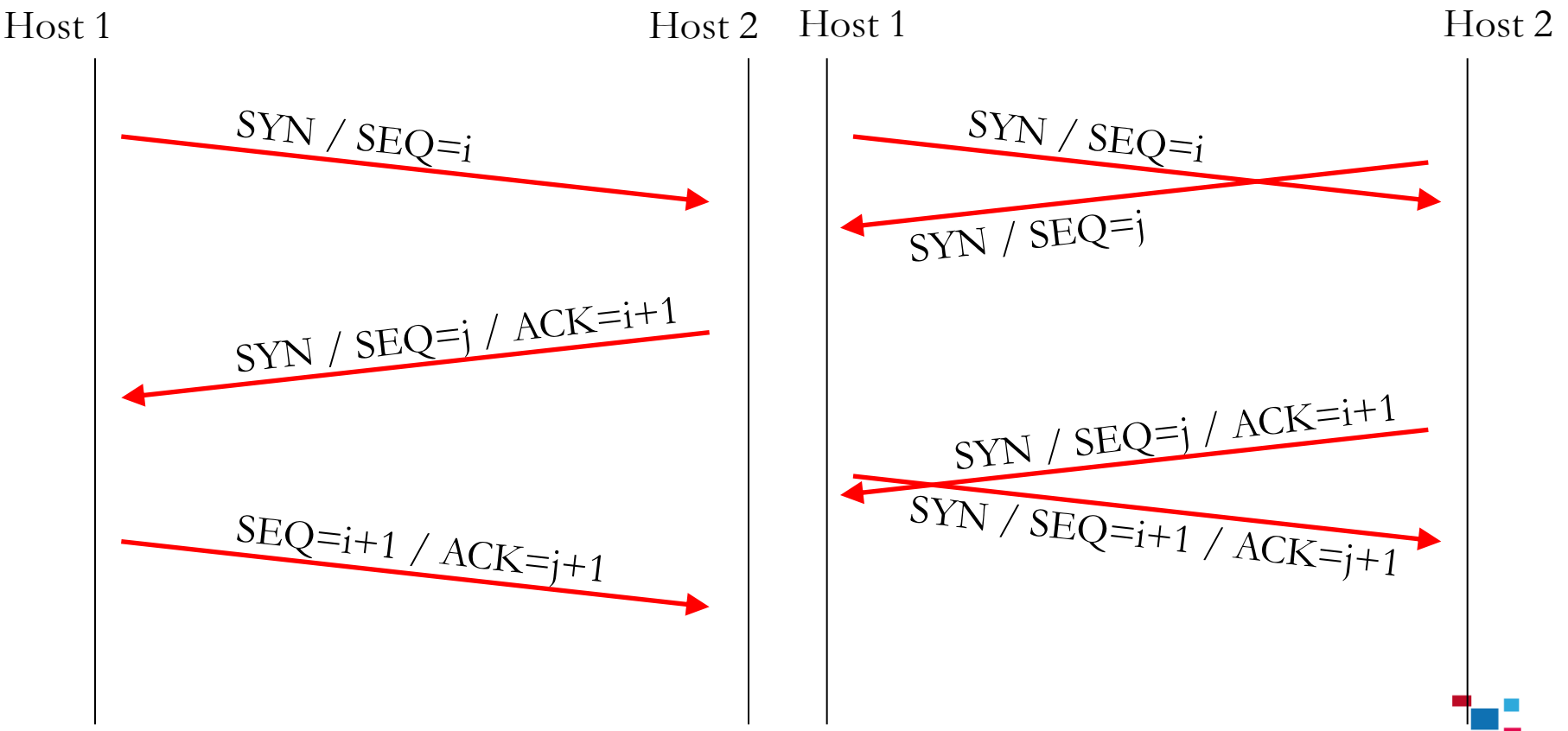
- Servicio de flujo fiable de bytes



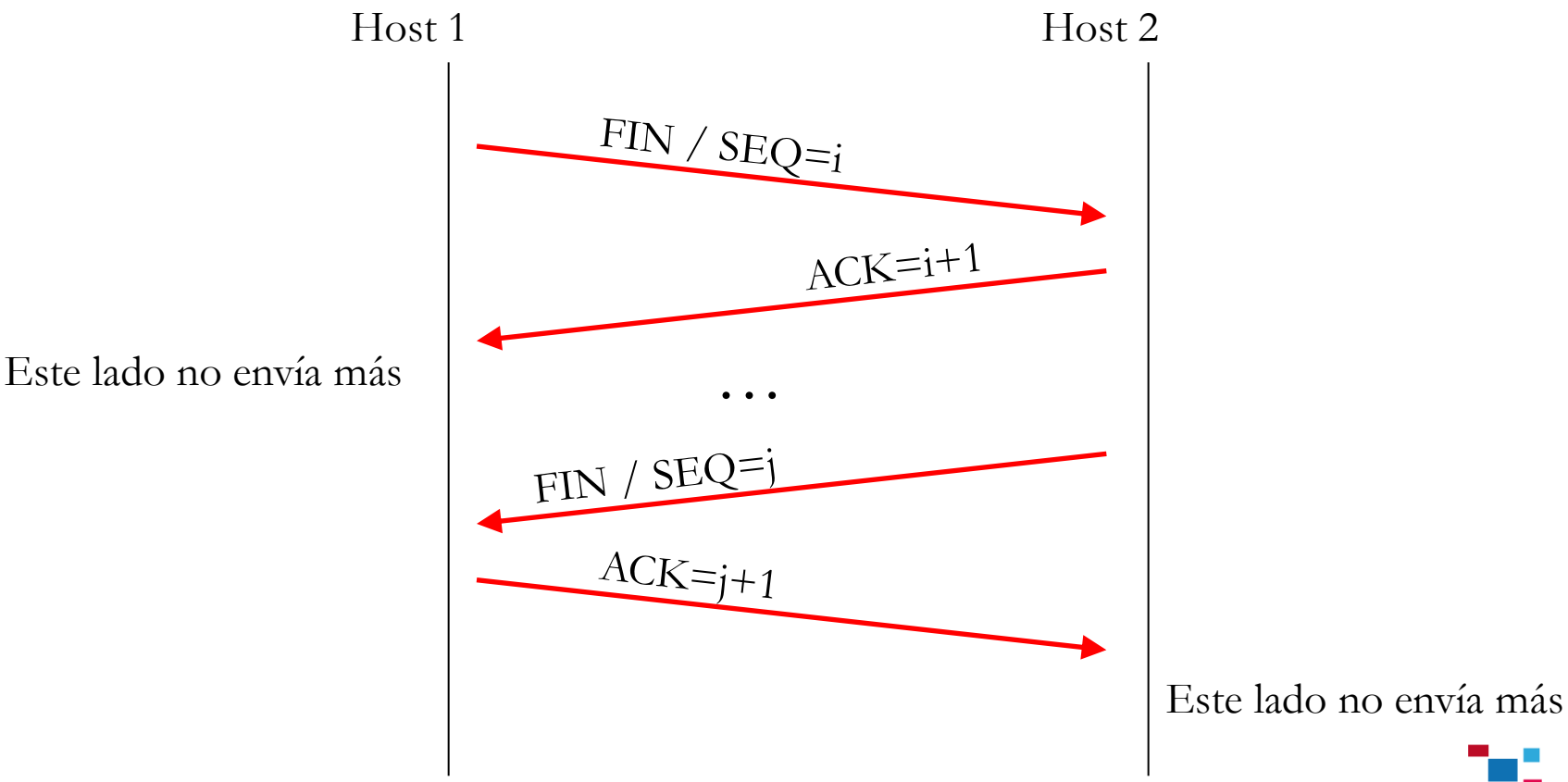
Números de secuencia



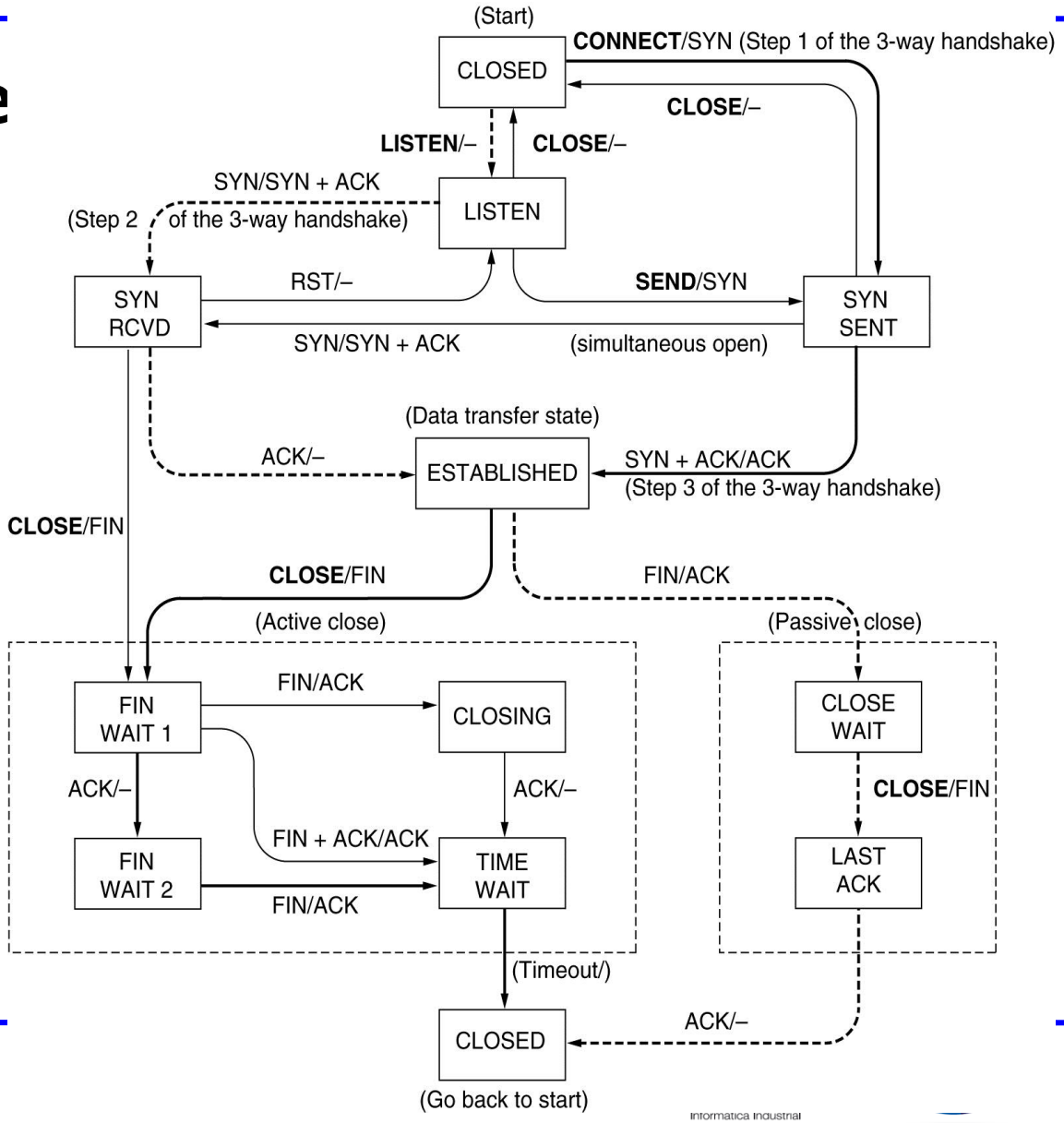
Apertura de la Conexión



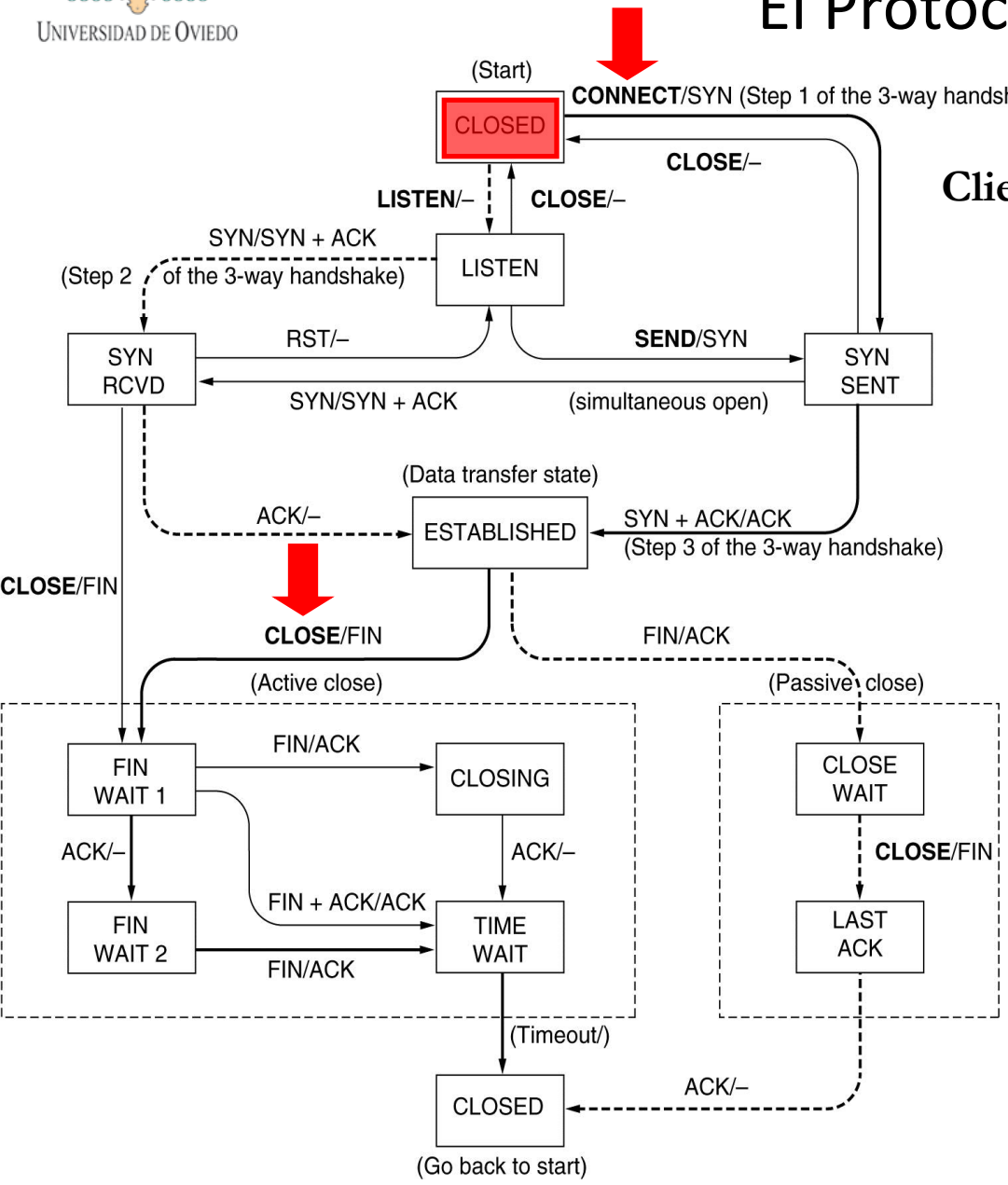
Cierre de la Conexión

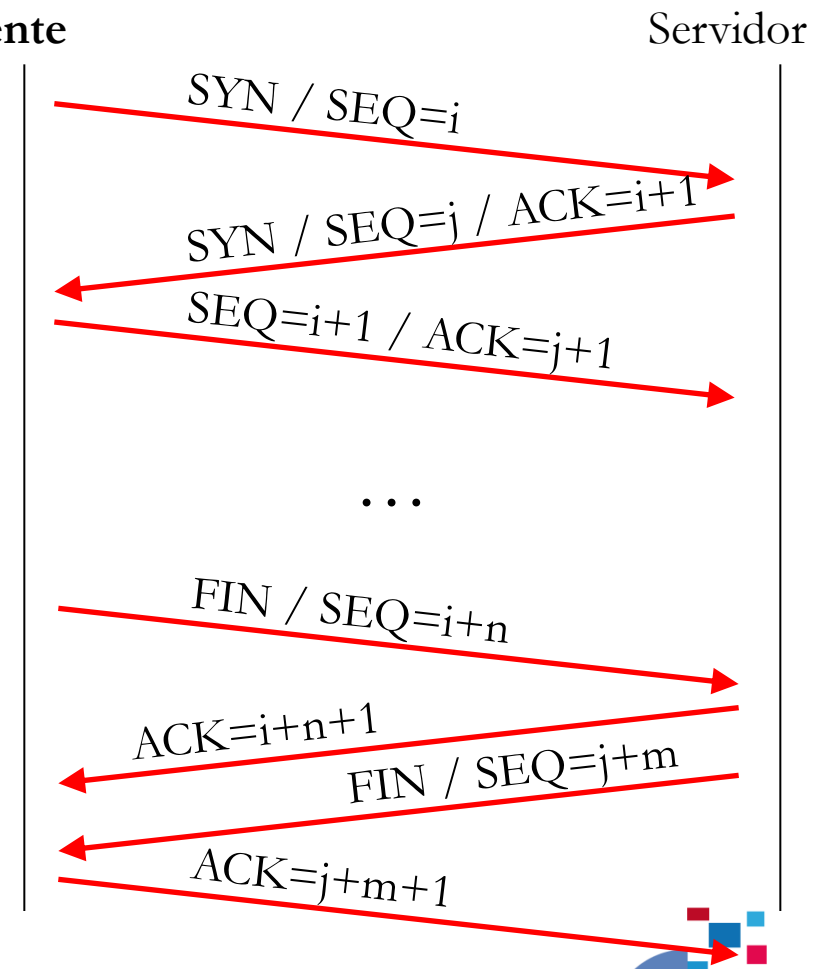


Administración de la Conexión

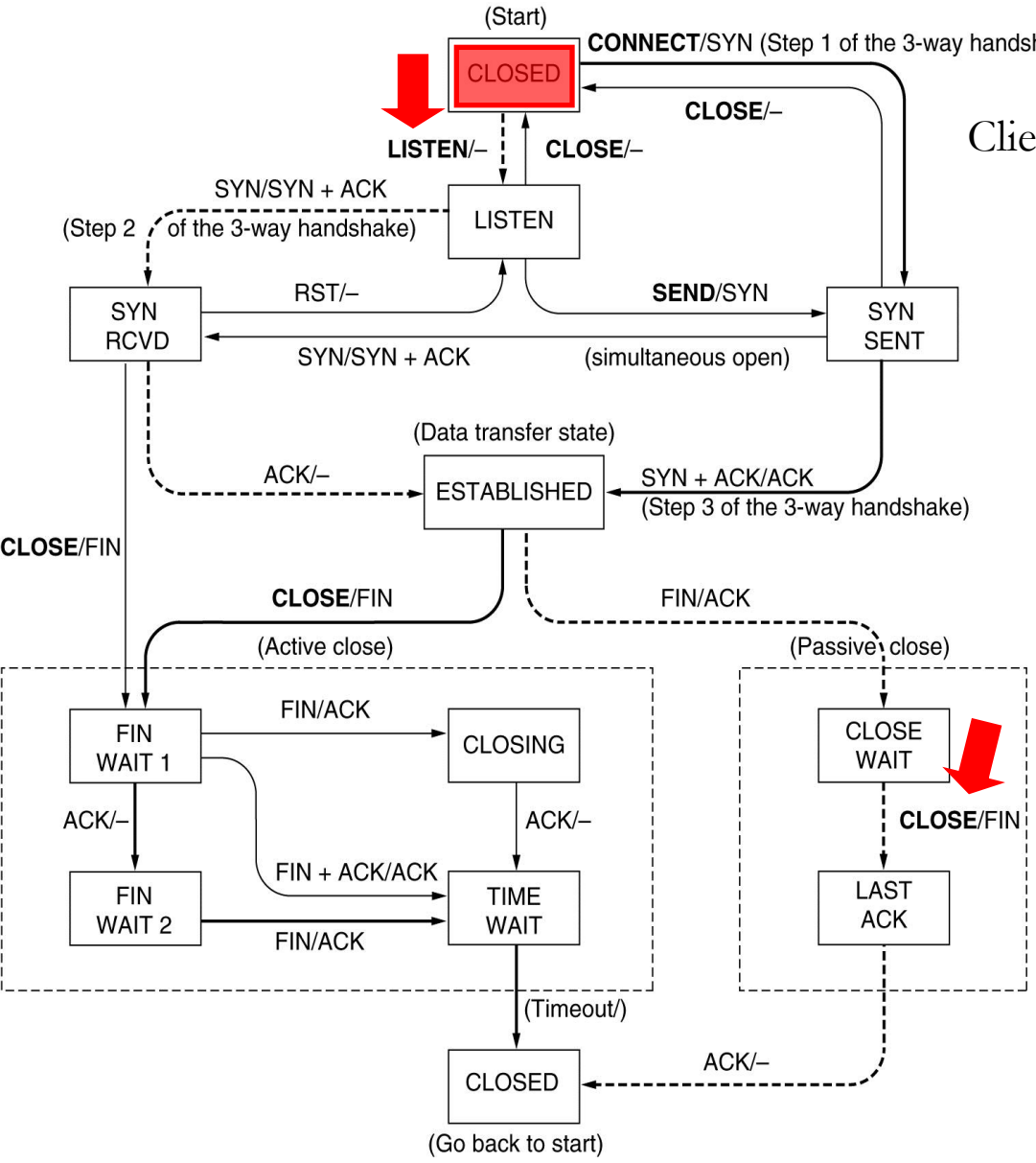


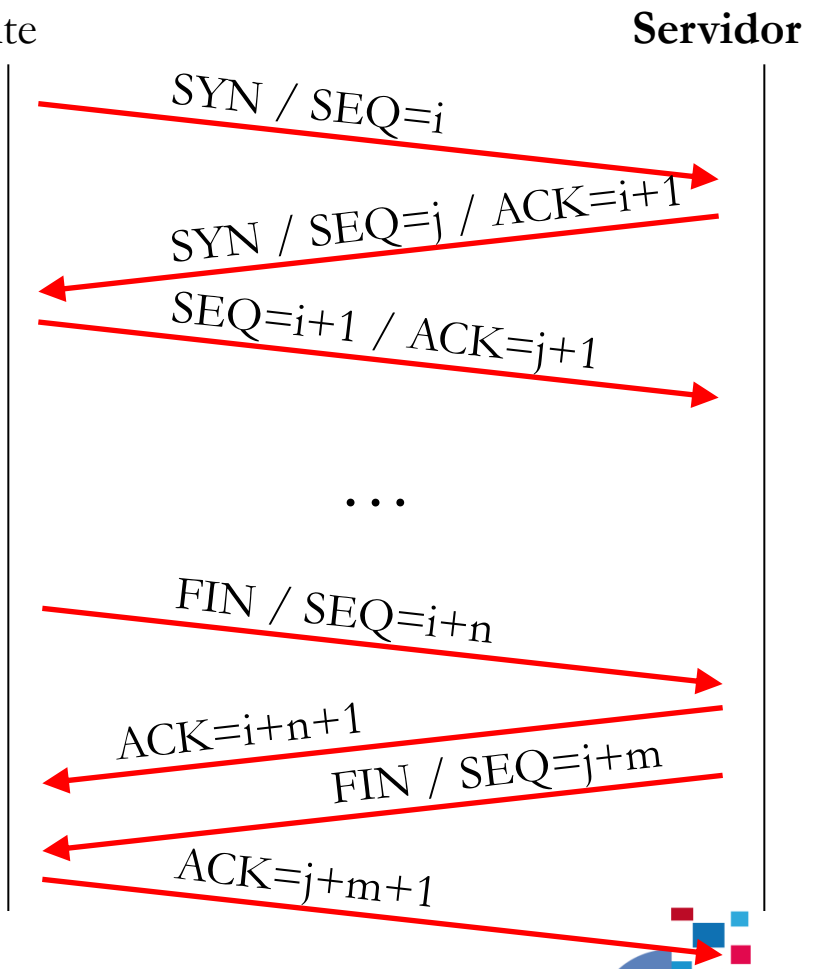
El Protocolo TCP



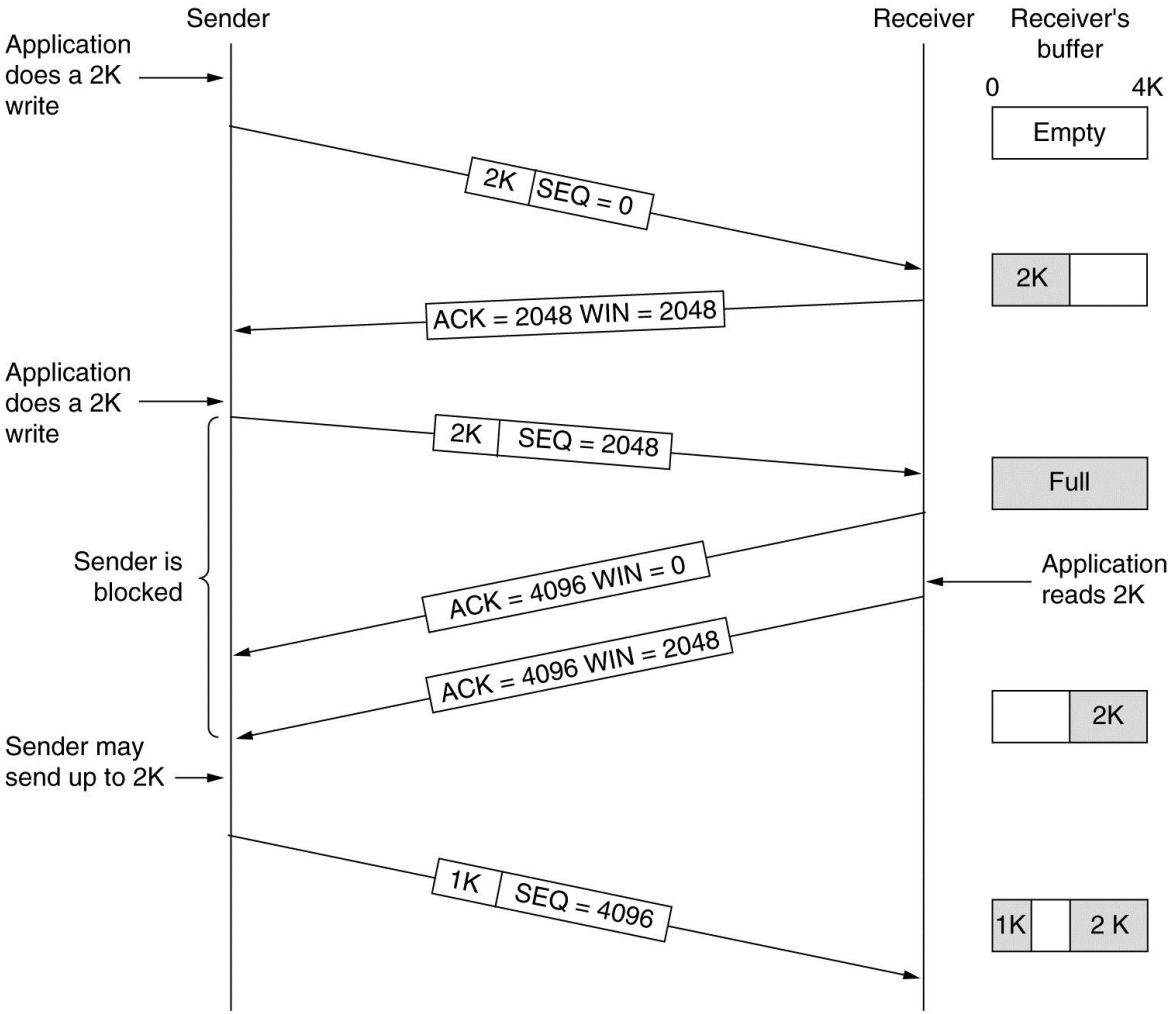


El Protocolo TCP



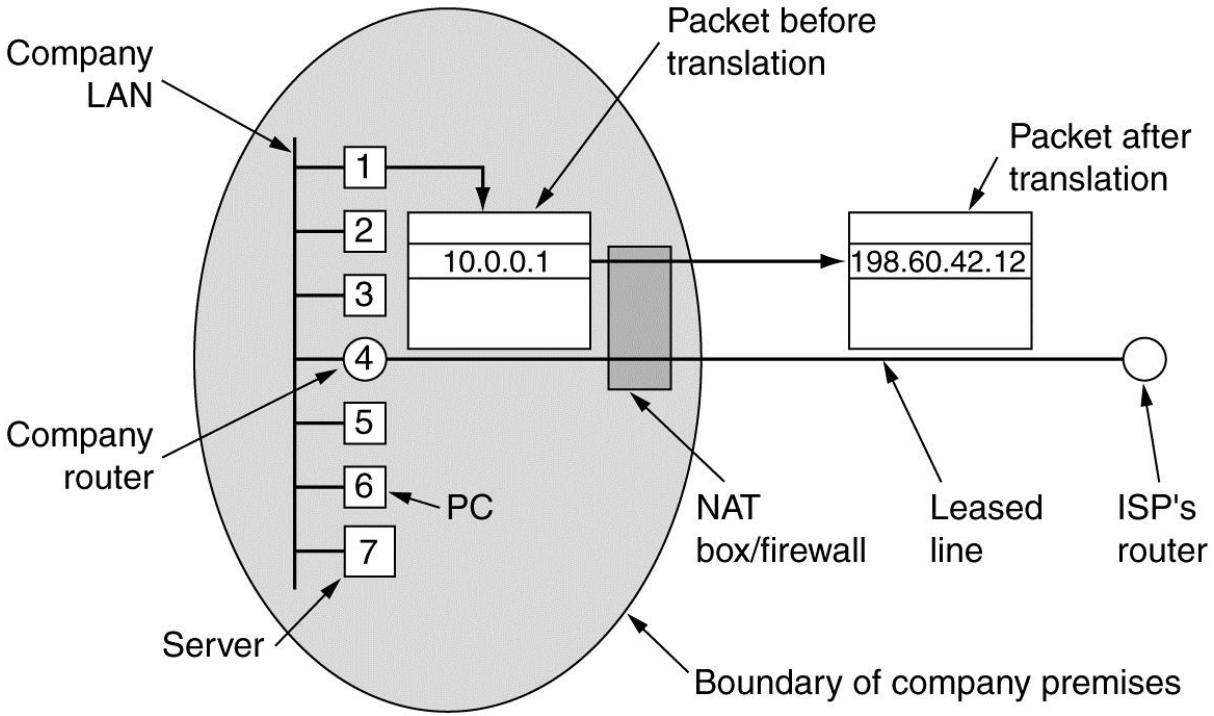


El Protocolo TCP



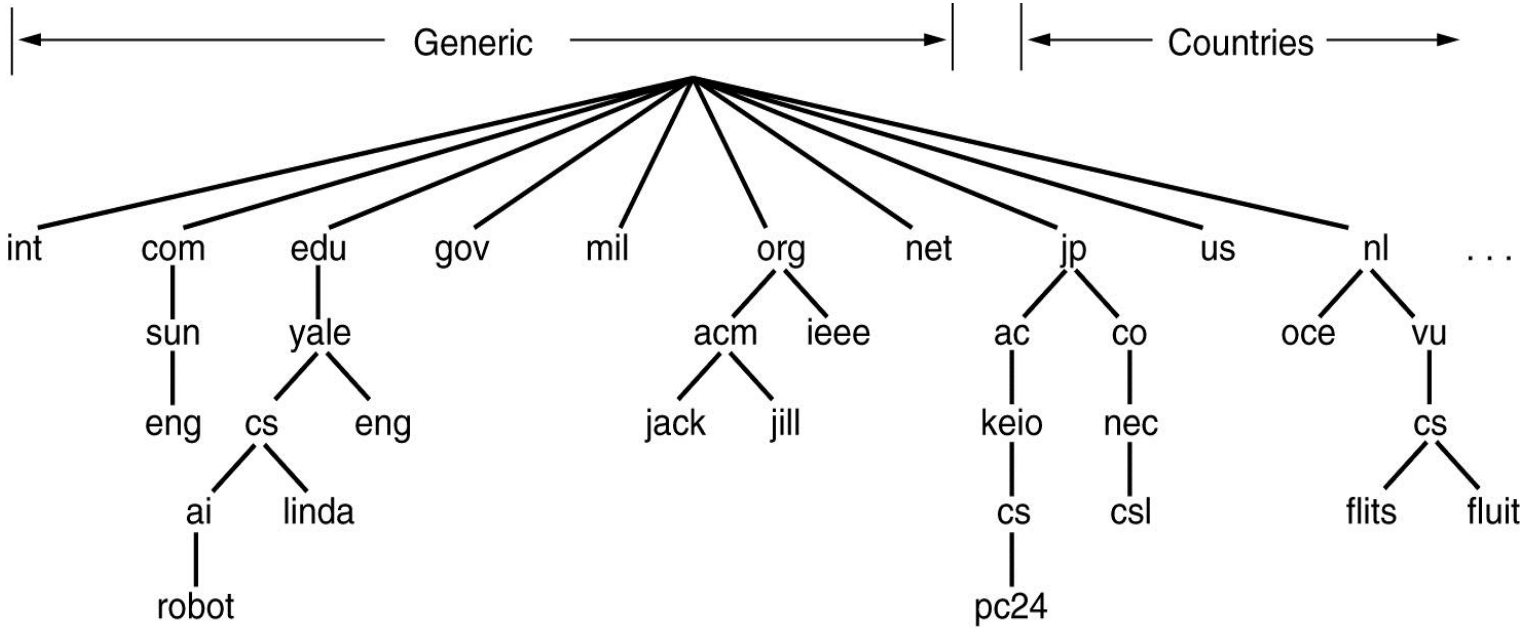
Network Address Translation – NAT

Esencia: Asignar una (o pocas) direcciones IP a redes locales que operen detrás de un encaminador especial y que permite solo conexiones **salientes**.



DNS (RFC 1034 y 1035)

Idea básica: Cada nodo tiene un nombre único asignado a una dirección IP. El Sistema de Nombres de Dominio (DNS) proporciona el servicio de búsqueda.



Un **nombre de dominio** es una ruta desde una hoja hasta la raíz. Un **dominio** es un subárbol en el **espacio de nombres de dominio**.

Registros de recursos

Cada **dominio** puede tener una serie de **recursos** asociados.

Tipo	Significado	Valor
SOA	Start Of Authority	Parámetros de zona
A	Dirección IP de un host	Entero de 32-bit
MX	Mail eXchange	Prioridad y dominio que acepta correo-e
NS	Name Server	Servidor de nombres de este dominio
CNAME	Nombre Canónico	Nombre del dominio
PTR	Pointer	Alias de una dirección IP
HINFO	Descripción del Host	CPU y SO (ASCII)
TXT	Texto	Texto ASCII no interpretado

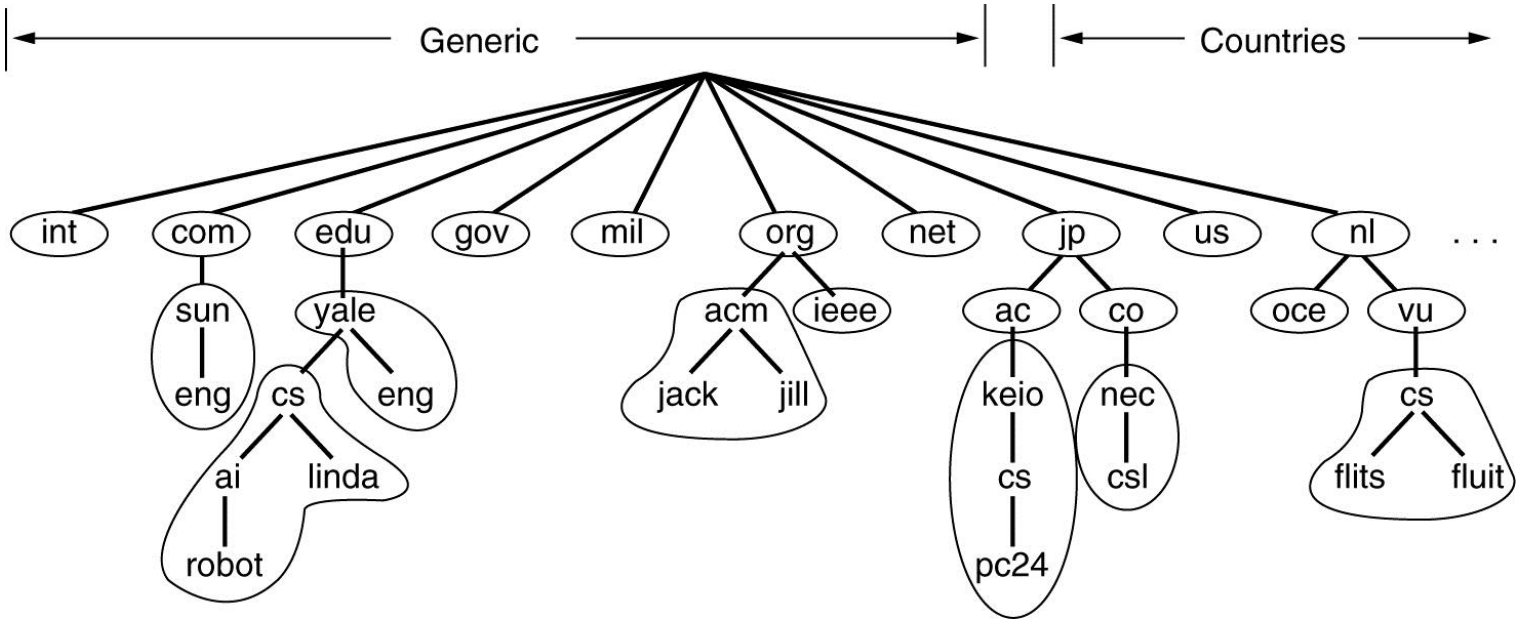
Registros de recursos: ejemplo

Una porción de la base de datos DNS en *cs.vu.nl*

```
; Authoritative data for cs.vu.nl
cs.vu.nl.        86400   IN   SOA      star boss (952771,7200,7200,2419200,86400)
cs.vu.nl.        86400   IN   TXT      "Divisie Wiskunde en Informatica."
cs.vu.nl.        86400   IN   TXT      "Vrije Universiteit Amsterdam."
cs.vu.nl.        86400   IN   MX       1 zephyr.cs.vu.nl.
cs.vu.nl.        86400   IN   MX       2 top.cs.vu.nl.

flits.cs.vu.nl.  86400   IN   HINFO    Sun Unix
flits.cs.vu.nl.  86400   IN   A        130.37.16.112
flits.cs.vu.nl.  86400   IN   A        192.31.231.165
flits.cs.vu.nl.  86400   IN   MX       1 flits.cs.vu.nl.
flits.cs.vu.nl.  86400   IN   MX       2 zephyr.cs.vu.nl.
flits.cs.vu.nl.  86400   IN   MX       3 top.cs.vu.nl.
www.cs.vu.nl.    86400   IN   CNAME    star.cs.vu.nl
ftp.cs.vu.nl.    86400   IN   CNAME    zephyr.cs.vu.nl

rowboat                  IN   A        130.37.56.201
                         IN   MX       1 rowboat
                         IN   MX       2 zephyr
                         IN   HINFO    Sun Unix

little-sister            IN   A        130.37.62.23
                         IN   HINFO    Mac MacOS

laserjet                 IN   A        192.31.231.216
                         IN   HINFO    "HP Laserjet IIISi" Proprietary
```

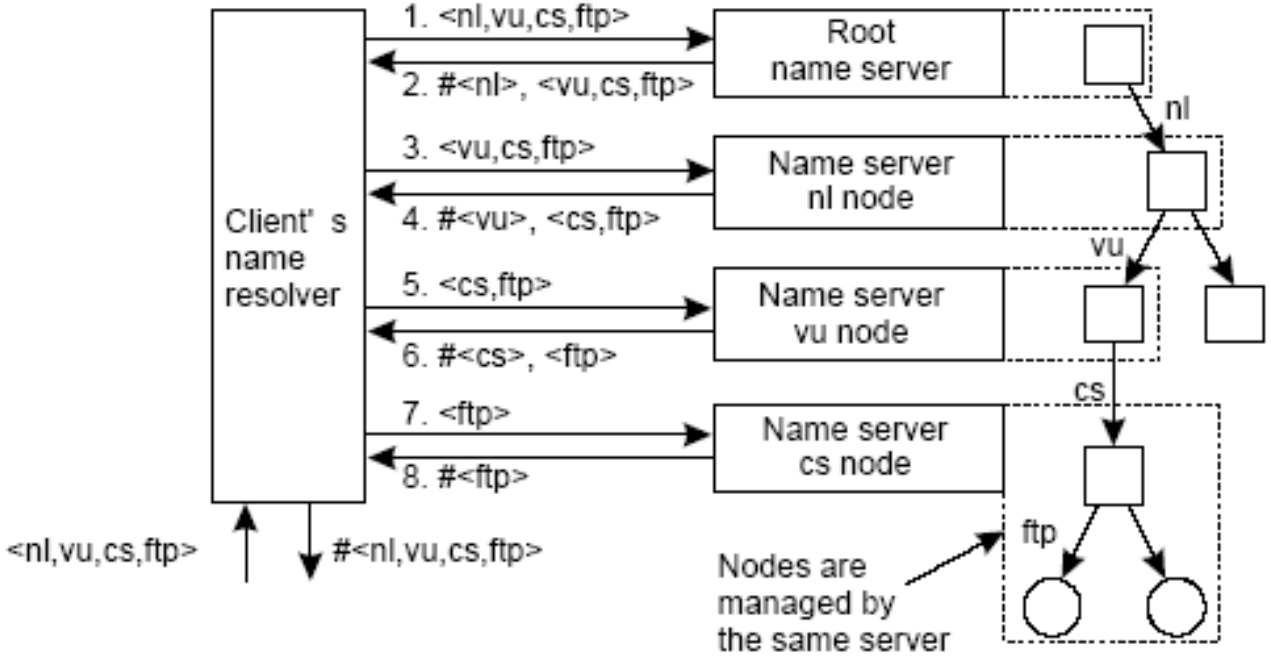
Servidores de Nombres DNS (I)

- Es imposible tener toda esta información en un solo servidor. Se implementa una solución distribuida y jerarquizada.
- **Idea básica:** Dividir el espacio de nombres en **zonas**, cada una de ellas con uno o más **servidores de nombres**.



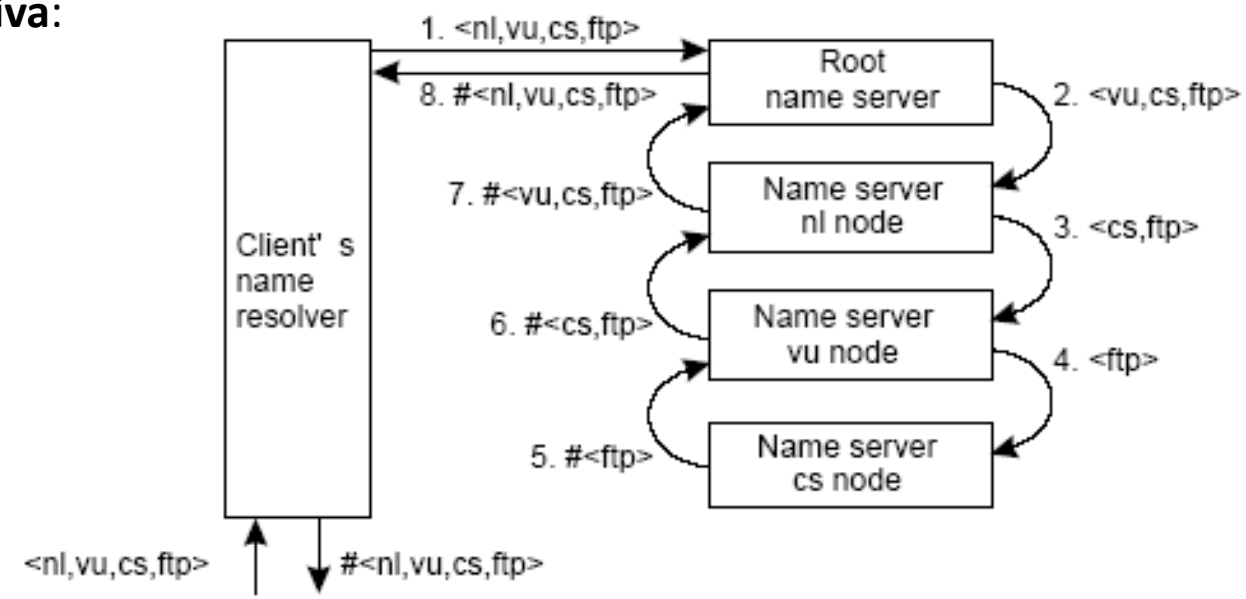
Servidores de Nombres DNS (II)

- Puede haber varios servidores por zona. Generalmente los servidores secundarios *secondary masters* obtienen la información de los primarios *primary masters*.
- Un **resolvedor** es un programa auxiliar que se ejecuta en la máquina de usuario y envía peticiones DNS a un servidor para obtener la información.
- Esta resolución puede ser **iterativa**:



Servidores de Nombres DNS (y III)

O **recursiva**:

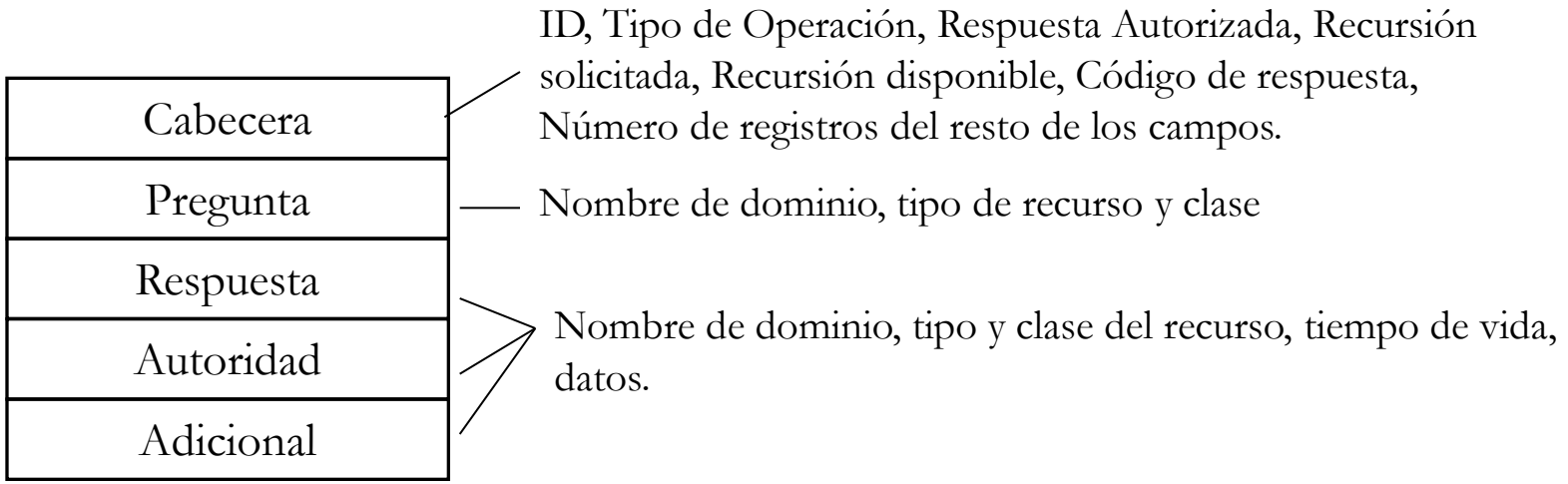


Esto no funcionaría (**¿por qué?**) si no fuese porque se supone que los emparejamientos nombre-dirección raramente cambian, por lo que pueden mantenerse en caché. Cuando un registro proviene directamente de la autoridad que administra el registro se denomina **registro autorizado**.

Protocolo DNS (RFC 1034)

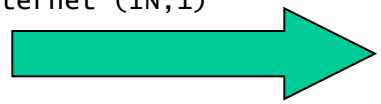
El protocolo DNS es muy sencillo (conceptualmente). Opera en dos modos:

- Búsqueda: utilizando UDP/53 (recomendado).
- Transferencias de zona: utilizando TCP/53 para la propagación de registros.



Ejemplo

```
IP D=[156.35.14.2] S=[156.35.152.99] LEN=39 ID=29991
UDP D=53 S=1030 LEN=39
DNS C ID=32115 OP=QUERY NAME=swcombine.com
...
DNS: Name = swcombine.com
DNS: Type = Host address (A,1)
DNS: Class = Internet (IN,1)
```

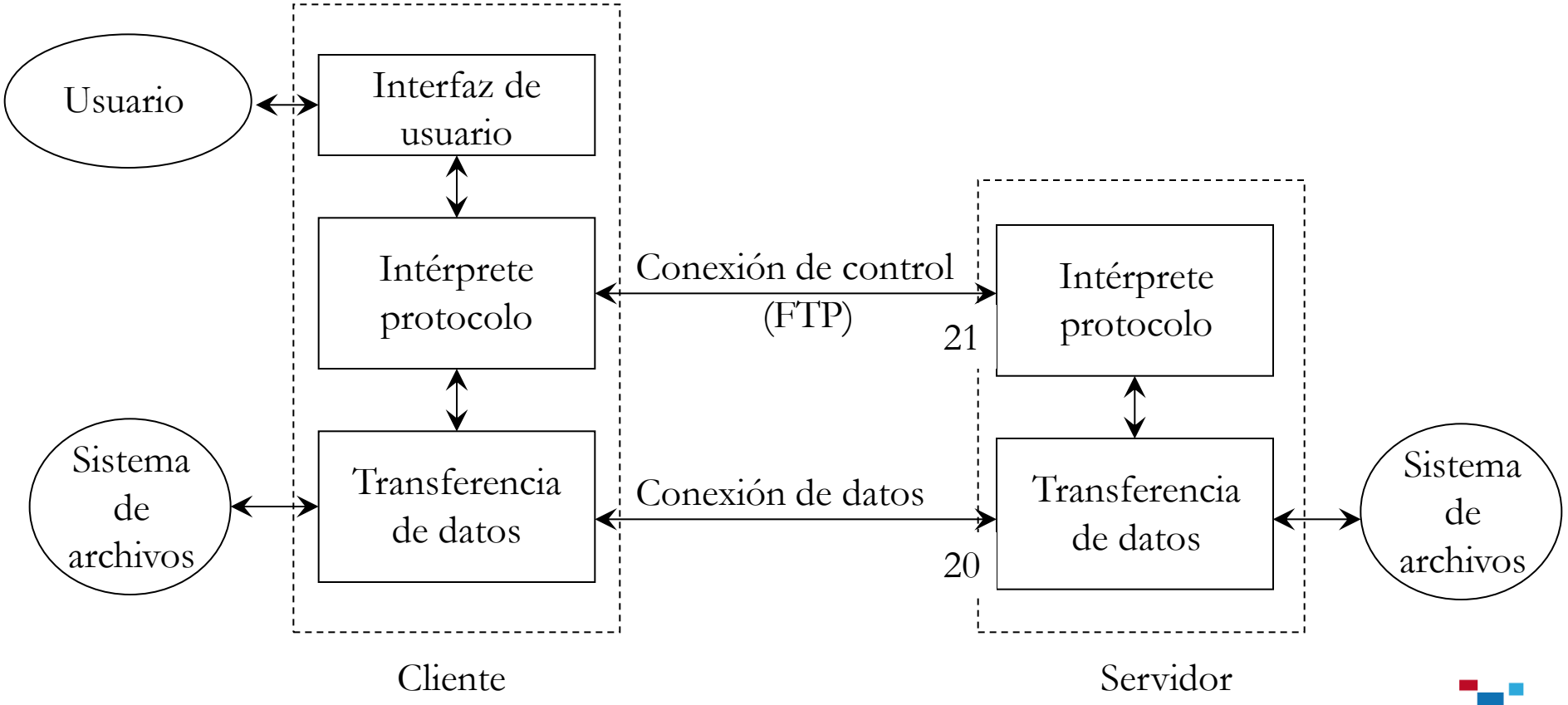


```
IP D=[156.35.152.99] S=[156.35.14.2] LEN=166 ID=19412
UDP D=1030 S=53 LEN=166
DNS R ID=32115 OP=QUERY RESPONSE STAT=OK NAME=swcombine.com
DNS: Not authoritative answer
...
DNS: Name = swcombine.com
DNS: Type = Host address (A,1)
DNS: Class = Internet (IN,1)
DNS: Time-to-live = 7200 (seconds)
DNS: Length = 4
DNS: Address = [72.249.7.125]

DNS: Authority section 1:
DNS: Name = swcombine.com
DNS: Type = Authoritative name server (NS,2)
DNS: Class = Internet (IN,1)
DNS: Time-to-live = 7200 (seconds)
DNS: Length = 20
DNS: Name server domain name = ns6.zoneedit.co.uk
...
```

Protocolo de Transferencia de Archivos – FTP (RFC 959)

- Protocolo simple (basado en texto) para la transferencia de archivos entre máquinas en Internet. Se ejecuta sobre TCP.
- Maneja la diversidad presente en las redes multiplataforma:
  - Distintas convenciones en los nombres de archivos (número de caracteres, extensiones, espacios,…).
  - Distinta codificación de los archivos (ASCII, EBCDIC, binario,…).
  - Acceso a directorios y permisos.
- FTP no proporciona ningún nivel de seguridad ni cifrado: nombres de usuario, claves y contenidos pueden ser husmeados, entre otros problemas.
- Alternativas seguras:
  - SFTP (FTP seguro sobre SSH-2)
  - FTPS (FTP sobre SSL)

FTP: Funcionamiento



Terminal Remoto – TELNET (RFC 854 y ss.)

- TELNET = TELetype NETwork
- Protocolo sencillo para acceder en modo terminal de texto a un sistema remoto.
- Utiliza una arquitectura cliente/servidor mediante TCP en el puerto 23.
- Maneja la diversidad en las capacidades del terminal que esté utilizando el usuario: manejar colores, posicionar el cursor, códigos ANSI,…
- Envía las pulsaciones de teclado que son interpretadas por el servidor y direccionadas al proceso remoto como si fuesen locales. Las respuestas son formateadas y enviadas al cliente.
- No implementa ningún mecanismo de seguridad.

TELNET: Funcionamiento