



**DECSAI**

**Departamento de Ciencias de la Computación e I.A.**

Universidad de Granada



# Internet: TCP/IP

Transmisión de datos y redes de ordenadores

# Internet: TCP/IP



La familia de protocolos TCP/IP

La capa de red en Internet

- El protocolo IP
- Protocolos auxiliares

La capa de transporte en Internet

- El protocolo TCP
- El protocolo UDP

La capa de aplicación en Internet

- El servicio de nombres DNS
- URLs [Uniform Resource Locators]
- Correo electrónico
- World Wide Web
- Aplicaciones multimedia



# Internet



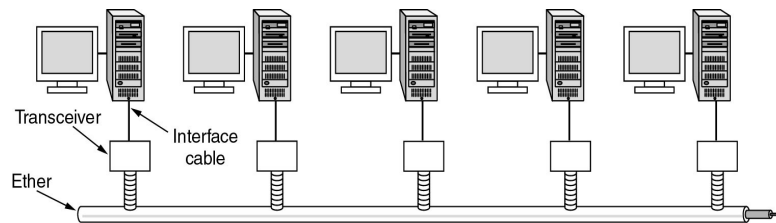
## Origen

Proyecto del US Defense Advanced Research Project Agency (DARPA) para el desarrollo de su red de conmutación de paquetes ARPANET.

## Objetivo

Tolerancia a errores en los elementos de la subred.

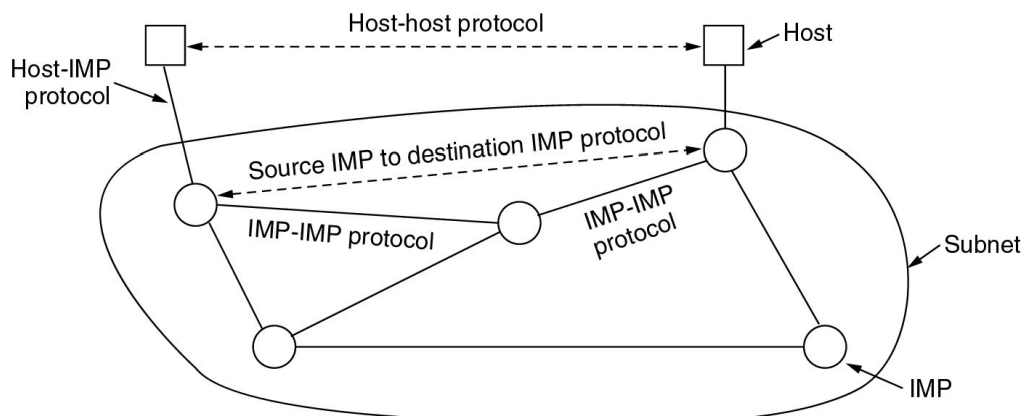
## Ethernet



# Internet



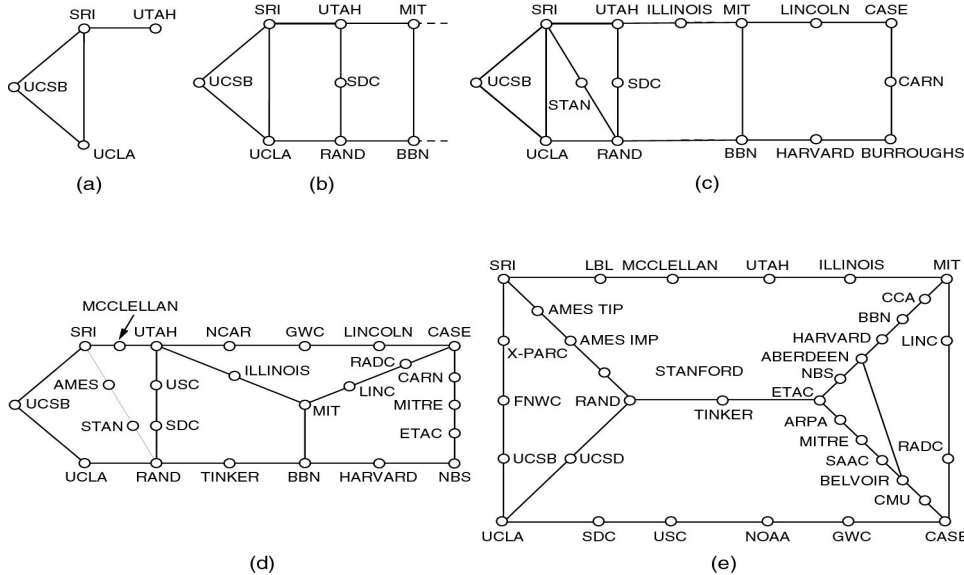
## Diseño original de ARPANET



# Internet



## Evolución de ARPANET



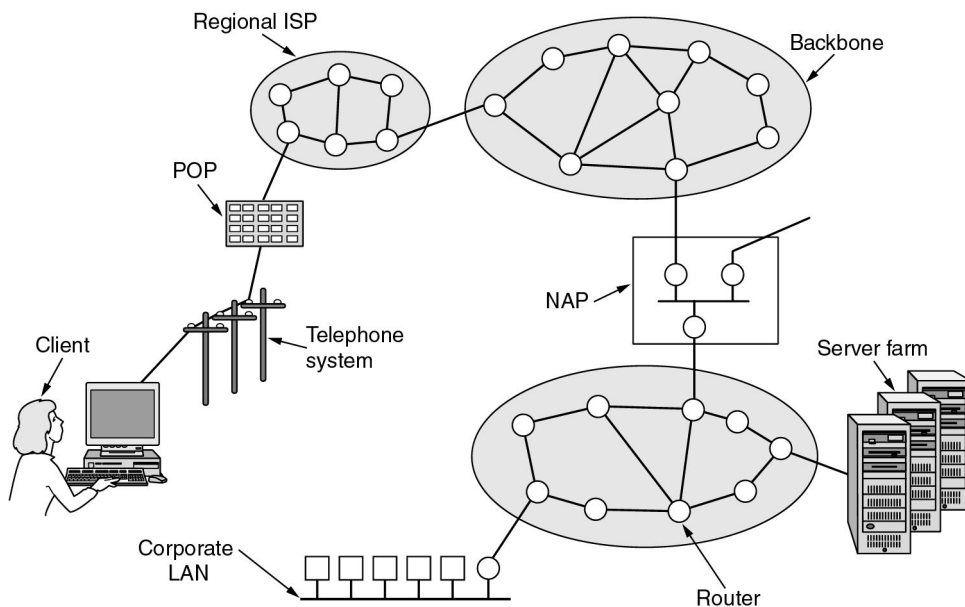
- (a) Diciembre 1969
- (b) Julio 1970
- (c) Marzo 1971
- (d) Abril 1972
- (e) Septiembre 1972



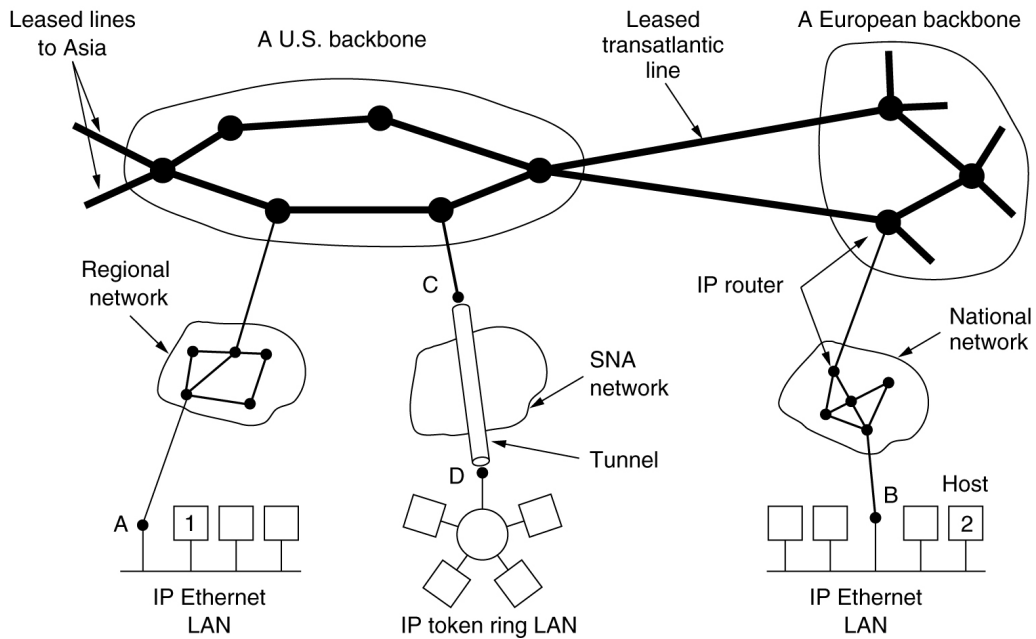
# Internet



## Arquitectura actual de Internet



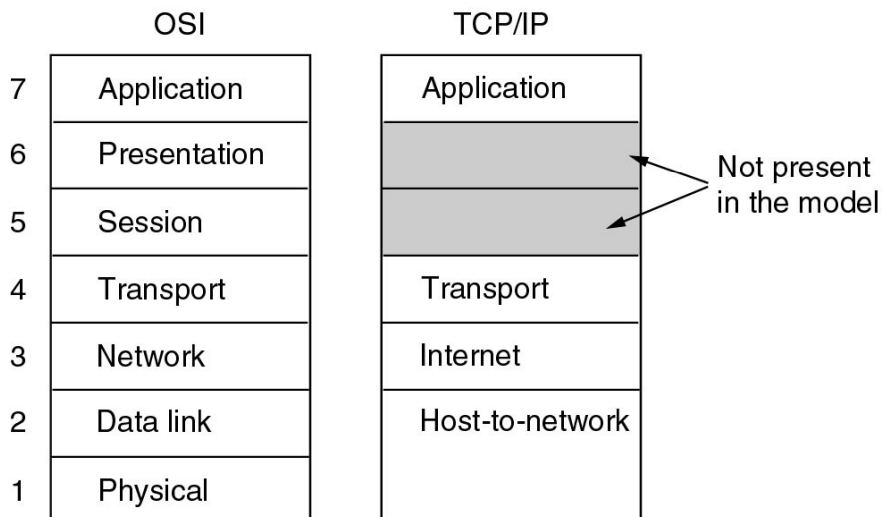
# Internet



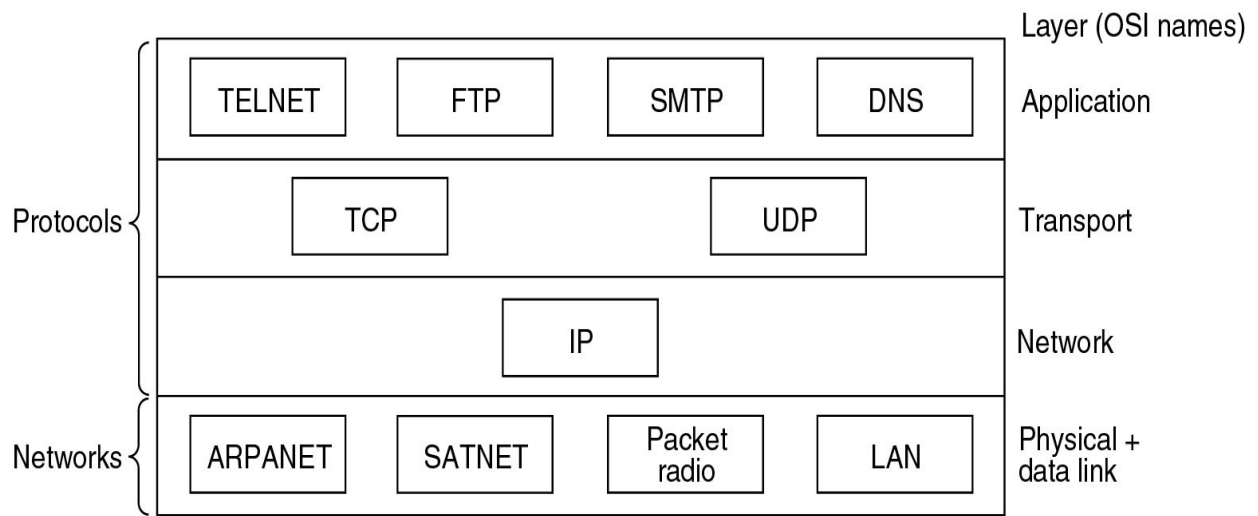
# El modelo TCP/IP



Estándar de facto



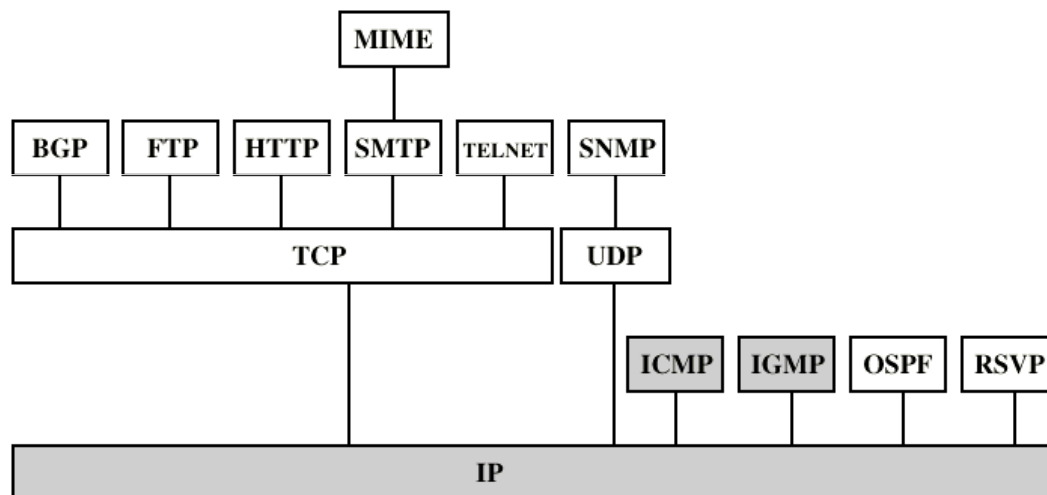
# El modelo TCP/IP



# El modelo TCP/IP



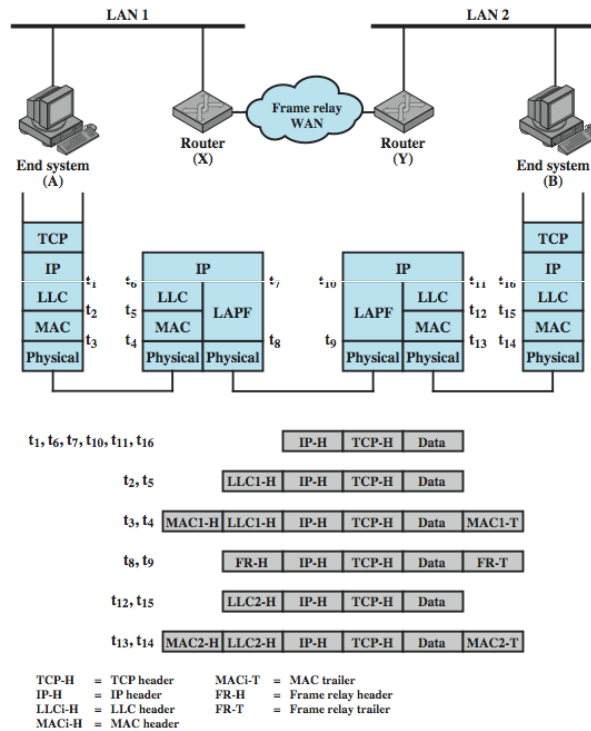
## La familia de protocolos TCP/IP



# El modelo TCP/IP



## Funcionamiento de Internet



# La capa de red



## Funciones de la capa de red en un sistema de comunicación

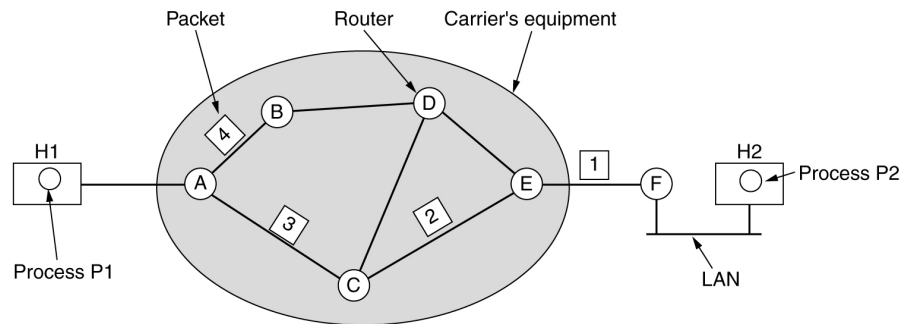
- Conmutación de paquetes
- Control de congestión
- Control del jitter
- Calidad de servicio (QoS)



# La capa de red



## Conmutación de paquetes



## Enrutamiento

A's table

	initially	later
A	-	-
B	B	B
C	C	C
D	B	B
E	C	B
F	C	B

Dest. Line

C's table

A	A
B	A
C	-
D	D
E	E
F	E

E's table

A	C
B	D
C	C
D	D
E	-
F	F

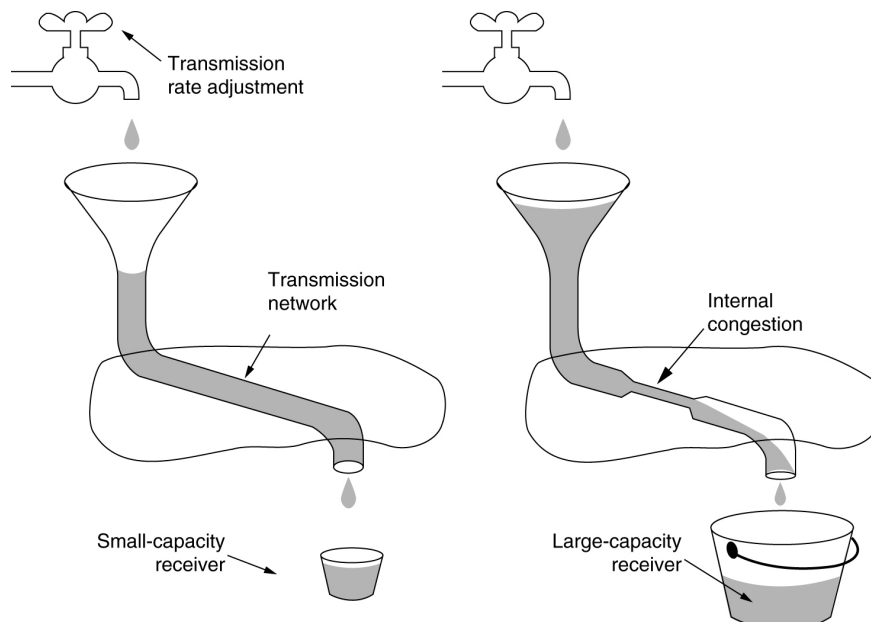


# La capa de red



## Control de congestión

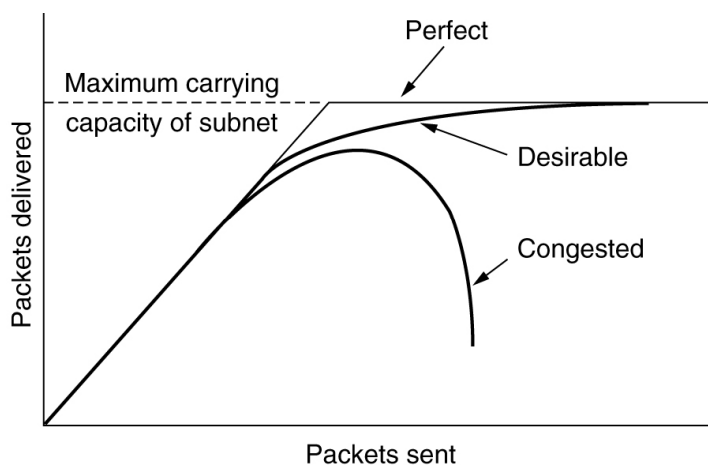
### Causas de la congestión



# La capa de red



## Control de congestión



### Principios básicos

- Monitorizar el funcionamiento del sistema para detectar la congestión.
- Transmitir información allá donde sea necesario actuar.
- Ajustar el funcionamiento del sistema para corregir el error.



# La capa de red



## Control de congestión

### Prevención de la congestión

Layer	Policies
Transport	<ul style="list-style-type: none"><li>• Retransmission policy</li><li>• Out-of-order caching policy</li><li>• Acknowledgement policy</li><li>• Flow control policy</li><li>• Timeout determination</li></ul>
Network	<ul style="list-style-type: none"><li>• Virtual circuits versus datagram inside the subnet</li><li>• Packet queueing and service policy</li><li>• Packet discard policy</li><li>• Routing algorithm</li><li>• Packet lifetime management</li></ul>
Data link	<ul style="list-style-type: none"><li>• Retransmission policy</li><li>• Out-of-order caching policy</li><li>• Acknowledgement policy</li><li>• Flow control policy</li></ul>

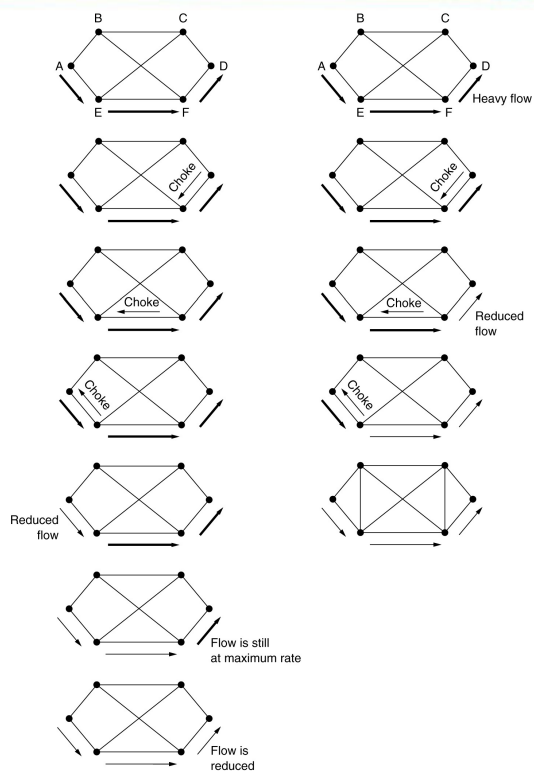




# La capa de red



## Control de congestión Paquetes de choque

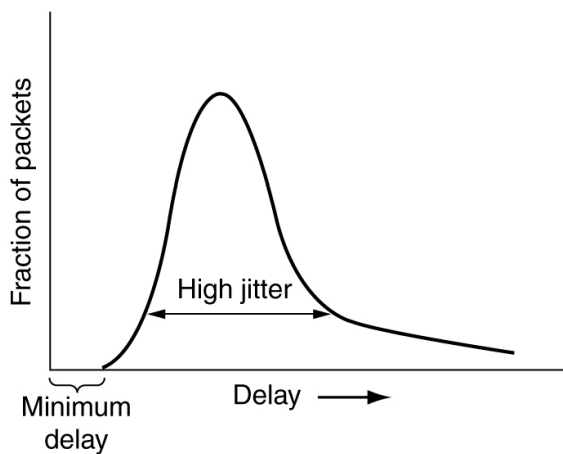


16

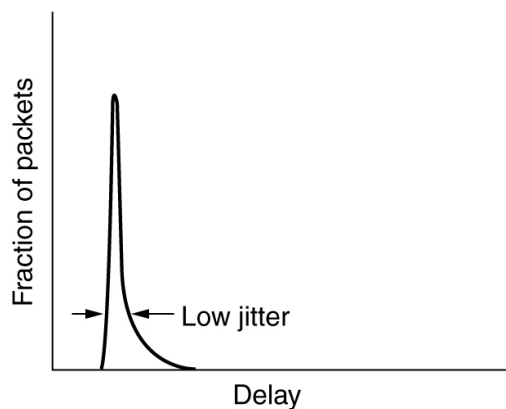
# La capa de red



## Control del jitter



Jitter elevado



Jitter reducido

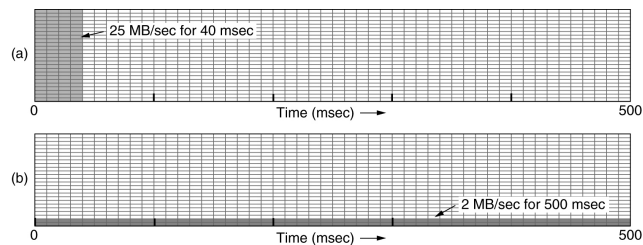
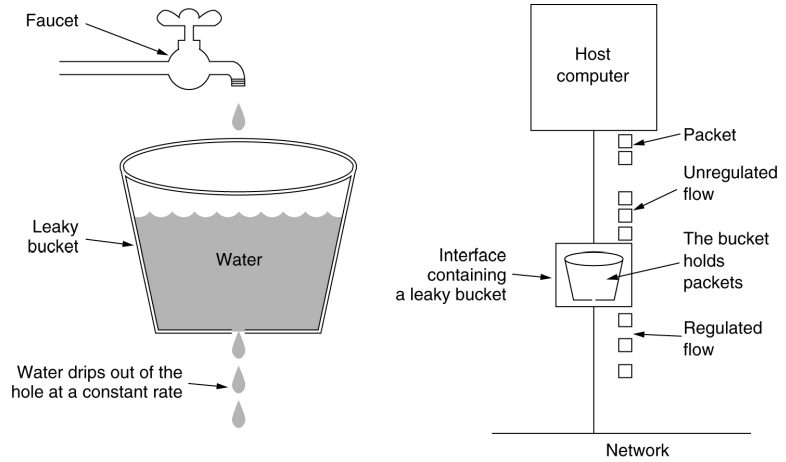


17

# La capa de red



## Control del jitter Leaky bucket



# La capa de red



## Calidad de servicio

### QoS [Quality of Service]

Application	Reliability	Delay	Jitter	Bandwidth
E-mail	High	Low	Low	Low
File transfer	High	Low	Low	Medium
Web access	High	Medium	Low	Medium
Remote login	High	Medium	Medium	Low
Audio on demand	Low	Low	High	Medium
Video on demand	Low	Low	High	High
Telephony	Low	High	High	Low
Videoconferencing	Low	High	High	High



# La capa de red



## Diferencias entre redes...

Item	Some Possibilities
Service offered	Connection oriented versus connectionless
Protocols	IP, IPX, SNA, ATM, MPLS, AppleTalk, etc.
Addressing	Flat (802) versus hierarchical (IP)
Multicasting	Present or absent (also broadcasting)
Packet size	Every network has its own maximum
Quality of service	Present or absent; many different kinds
Error handling	Reliable, ordered, and unordered delivery
Flow control	Sliding window, rate control, other, or none
Congestion control	Leaky bucket, token bucket, RED, choke packets, etc.
Security	Privacy rules, encryption, etc.
Parameters	Different timeouts, flow specifications, etc.
Accounting	By connect time, by packet, by byte, or not at all

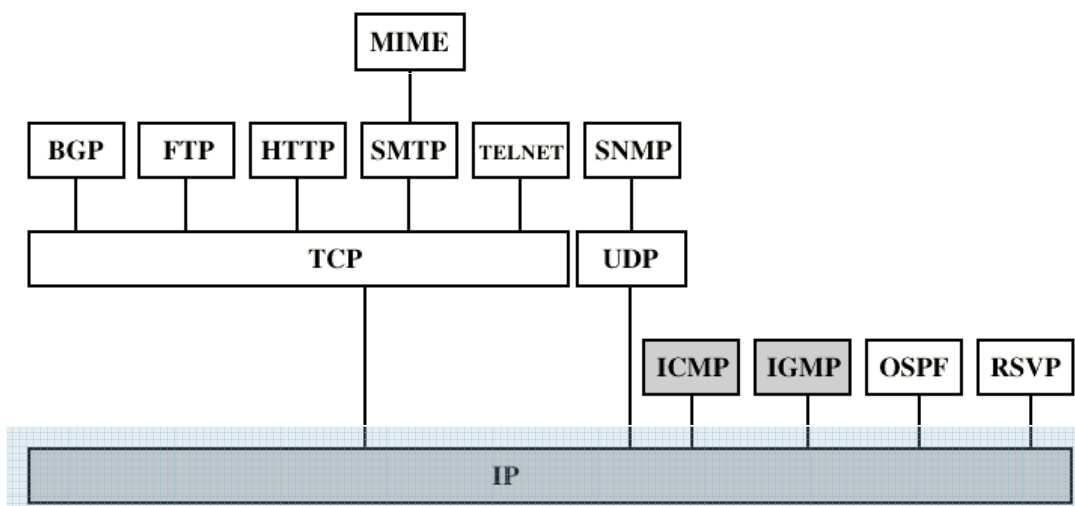


# El protocolo IP



## IP [Internet Protocol]

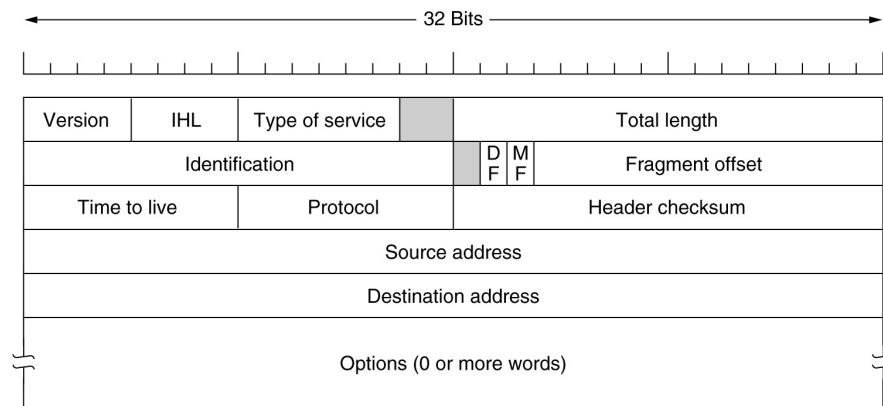
### La capa de red en Internet



# El protocolo IP



## Cabecera del datagrama IPv4



Campos:

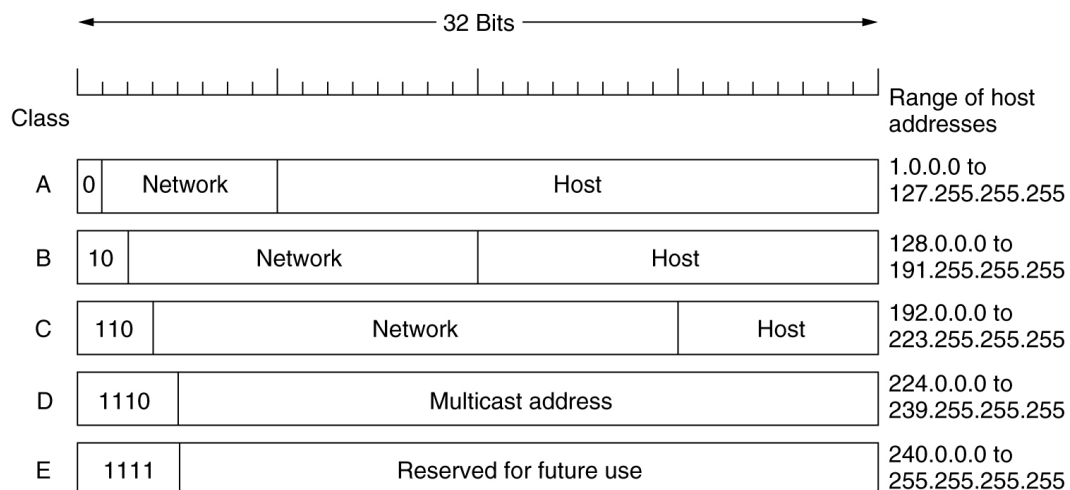
Versión (IPv4), IHL (Internet Header Length, en palabras de 32 bits), tipo de servicio (precedencia), longitud del datagrama (en octetos), identificación (número de secuencia), flags (don't fragment & more fragments), offset, TTL (time to live), protocolo (p.ej. TCP), checksum de la cabecera, direcciones IP del emisor y del destinatario, opciones (source routing, timestamps...).



# El protocolo IP



## Direcciones IP



# El protocolo IP



## Direcciones IP

### Direcciones especiales

0 0		This host		
0 0	...	0 0	Host	A host on this network
1 1				Broadcast on the local network
Network	1 1 1 1	...	1 1 1 1	Broadcast on a distant network
127	(Anything)			Loopback

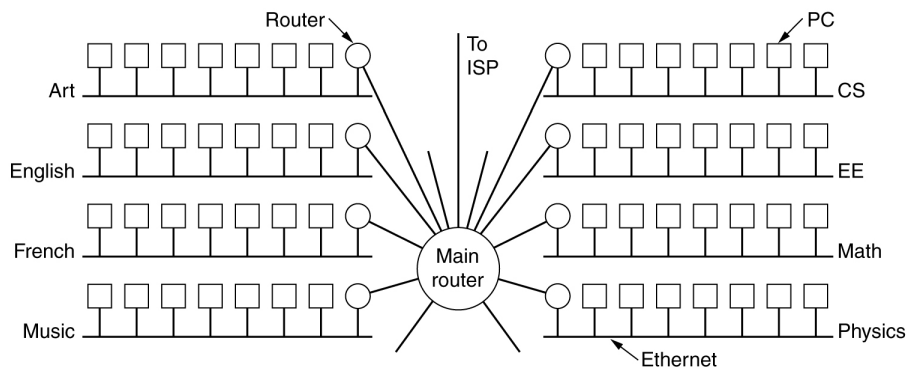


# El protocolo IP



## Direcciones IP

### Subredes



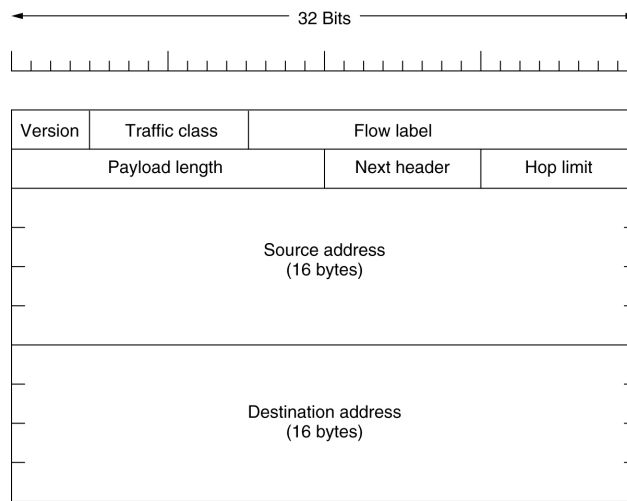
Subnet	10	Network	Subnet	Host	
mask	1 0 0 0 0 0 0 0 0 0 0 0 0				



# El protocolo IP



## El protocolo IPv6 = IPng [IP Next Generation]



- Ampliación del espacio de direcciones (128 bits).
- Tres tipos de direcciones: Unicast, anycast y multicast.



# El protocolo IP

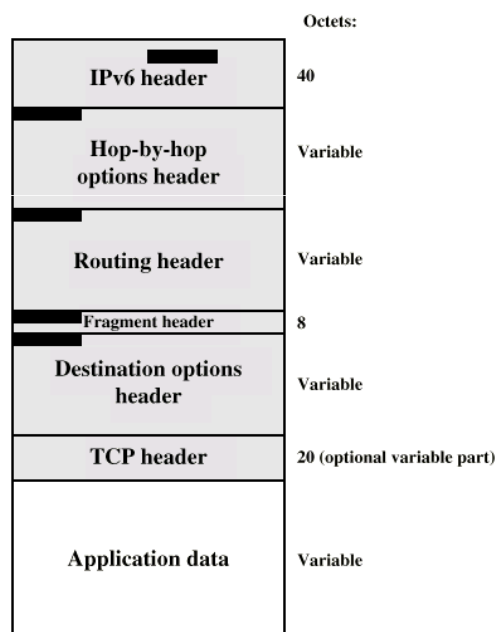


## El protocolo IPv6 = IPng [IP Next Generation]

- Cabeceras opcionales

Entre la cabecera IPv6 y la de la capa de transporte, para dar soporte a nuevos tipos de servicio.

p.ej. Vídeo en tiempo real...



█ = Next Header field





## El protocolo ICMP

### [Internet Control Message Protocol]

RFC 792: Control de flujo (paquetes de choque), eco (ping), time to live.

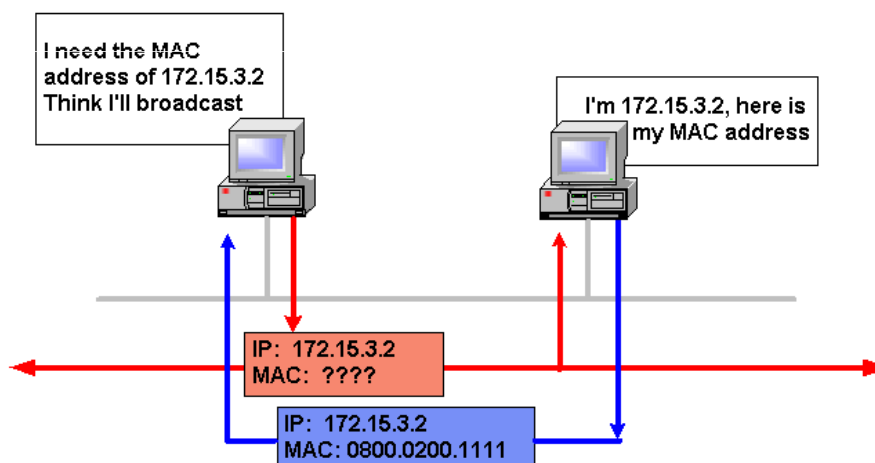
Message type	Description
Destination unreachable	Packet could not be delivered
Time exceeded	Time to live field hit 0
Parameter problem	Invalid header field
Source quench	Choke packet
Redirect	Teach a router about geography
Echo request	Ask a machine if it is alive
Echo reply	Yes, I am alive
Timestamp request	Same as Echo request, but with timestamp
Timestamp reply	Same as Echo reply, but with timestamp



## El protocolo ARP

### [Address Resolution Protocol]

- Conversión de direcciones IP a direcciones MAC



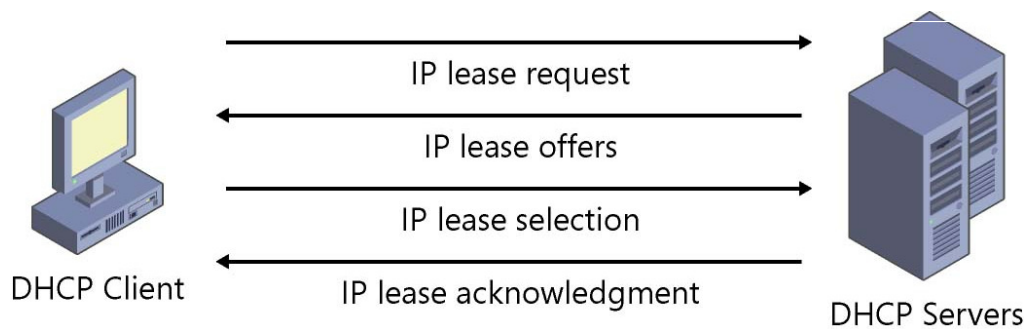
# Protocolos auxiliares



## El protocolo DHCP

### [Dynamic Host Configuration Protocol]

- Asignación dinámica de direcciones IP



“¿Qué dirección IP utilizo?”

“Tu dirección IP es 192.168.1.10”



# Protocolos auxiliares



## El protocolo IGMP

### [Internet Group Management Protocol]

- RFC 1112: Gestión de grupos para multicasting

## El protocolo RSVP

### [Resource reSerVation Protocol]

- RFC 2205: Reserva de recursos (QoS)

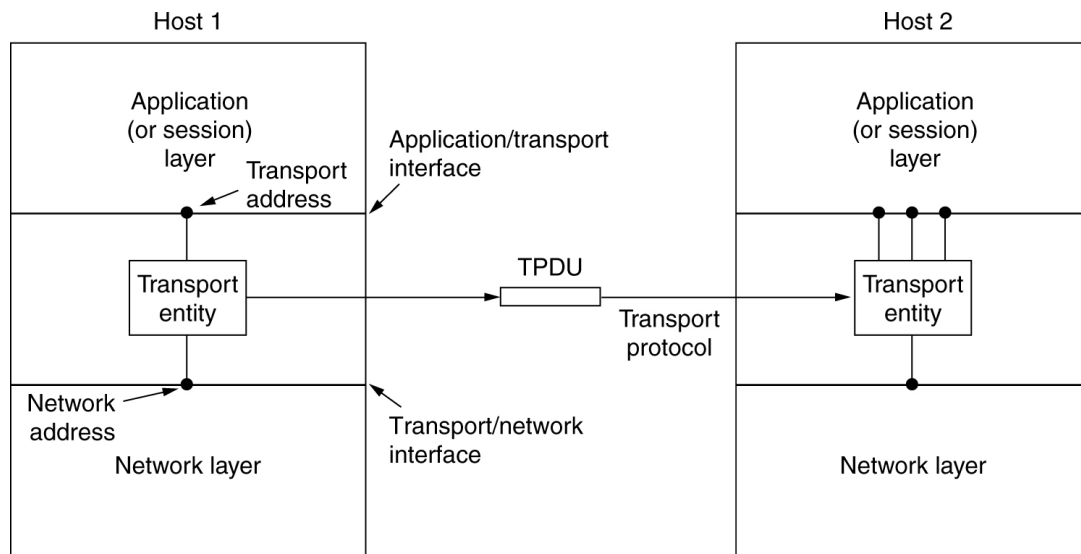
## Protocolos de enrutamiento

- OSPF [Open Shortest Path First]
- BGP [Border Gateway Protocol]





# La capa de transporte



Las capas de red, transporte y aplicación



# La capa de transporte



## Servicios proporcionados a la capa de aplicación

- Servicios orientados a conexión
- Servicios no orientados a conexión

## Funciones de la capa de transporte

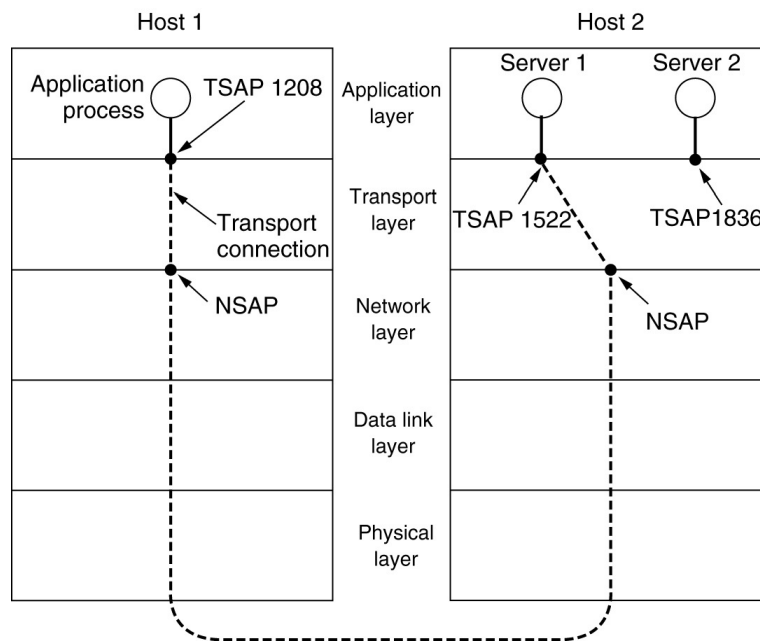
- Direccionamiento y multiplexación.
- Control de flujo de extremo a extremo (entrega ordenada y retransmisión).
- Establecimiento y liberación de conexiones (para servicios orientados a conexión).



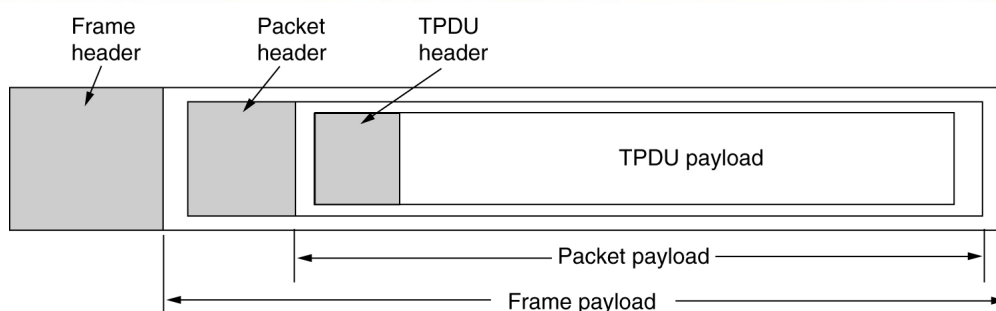
# La capa de transporte



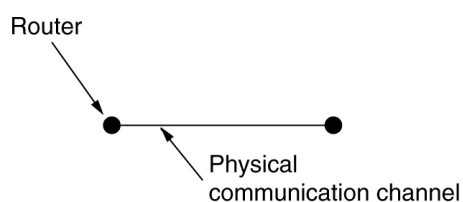
## Direccionamiento y multiplexación



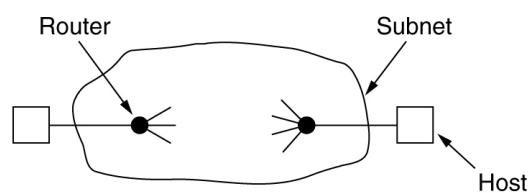
# La capa de transporte



## La capa de transporte vs. La capa de enlace de datos



Capa de enlace de datos



Capa de transporte



# La capa de transporte



## La capa de transporte en Internet

- **El protocolo TCP**  
[Transmission Control Protocol]  
Servicios orientados a conexión.
- **El protocolo UDP**  
[User Datagram Protocol]  
Servicios no orientados a conexión.

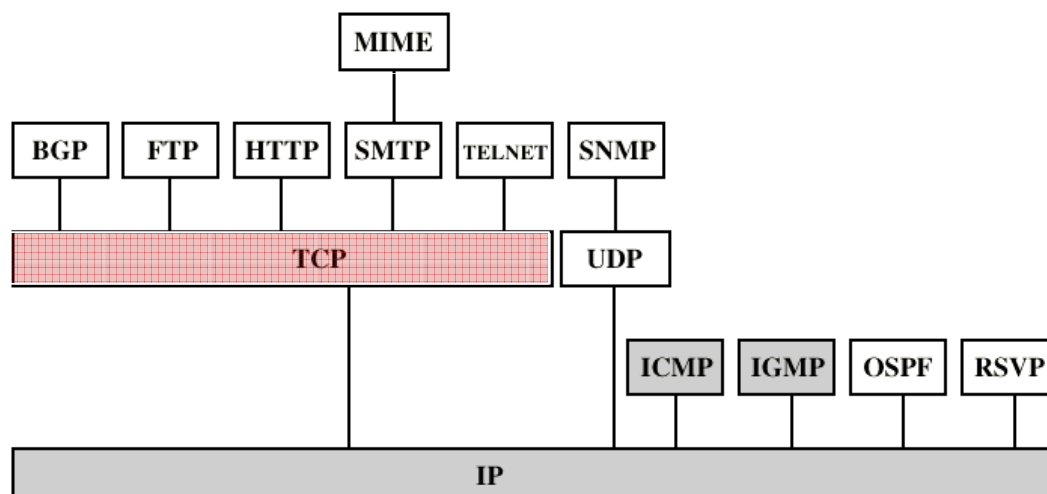


# El protocolo TCP



## Transmission Control Protocol

RFC 793: Servicios orientados a conexión



# El protocolo TCP



## Primitivas de servicio: Sockets

Primitiva	Uso
SOCKET	Crear un extremo [end point] de la comunicación .
BIND	Asociar una dirección local a un socket (IP:puerto).
LISTEN	Anunciar la disponibilidad para aceptar conexiones.
ACCEPT	Bloquear el servidor hasta que llegue una solicitud de conexión.
CONNECT	Intentar establecer una conexión.
SEND	Enviar datos a través de la conexión.
RECEIVE	Recibir datos provenientes de la conexión.
CLOSE	Cerrar la conexión.



# El protocolo TCP



## Multiplexación de conexiones: Puertos

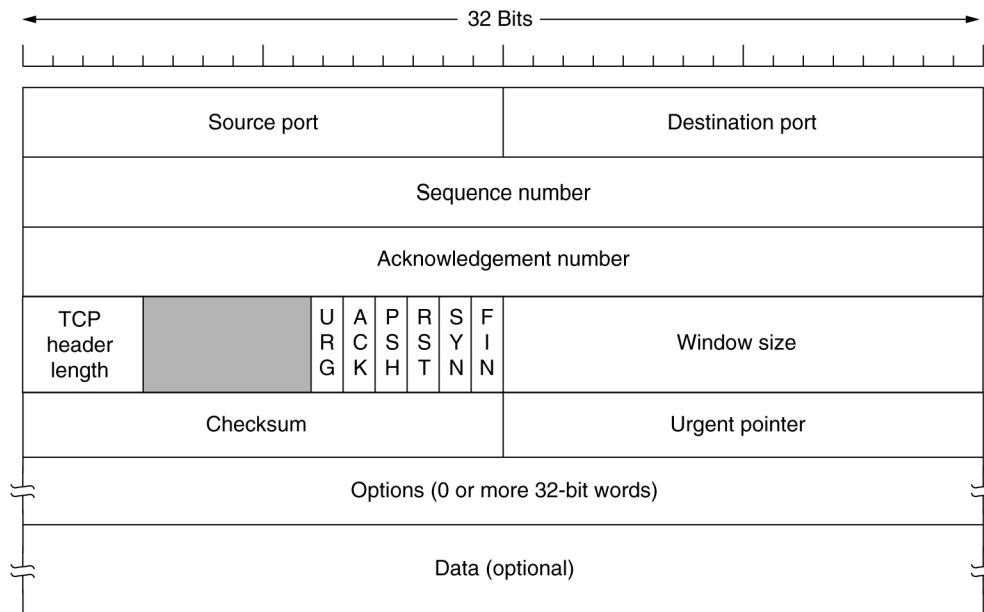
Puerto	Protocolo	Uso
21	FTP	Transferencia de ficheros
23	Telnet	Acceso remoto
25	SMTP	Correo electrónico
79	Finger	Información acerca de usuarios
80	HTTP	World Wide Web
110	POP3	Correo electrónico
119	NNTP	Grupos de noticias USENET
...	...	...



# El protocolo TCP



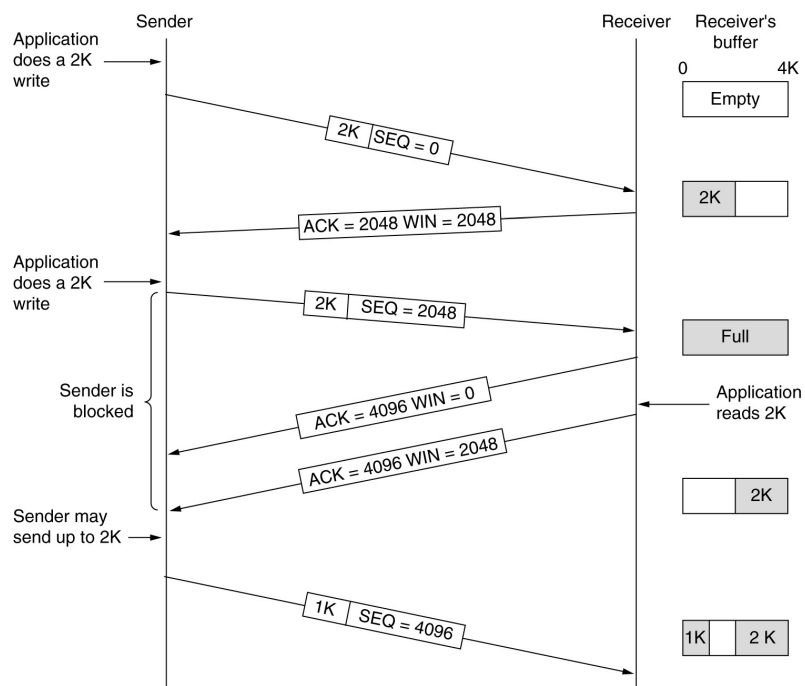
## Cabecera del segmento TCP



# El protocolo TCP



## Control de flujo mediante ventana deslizante



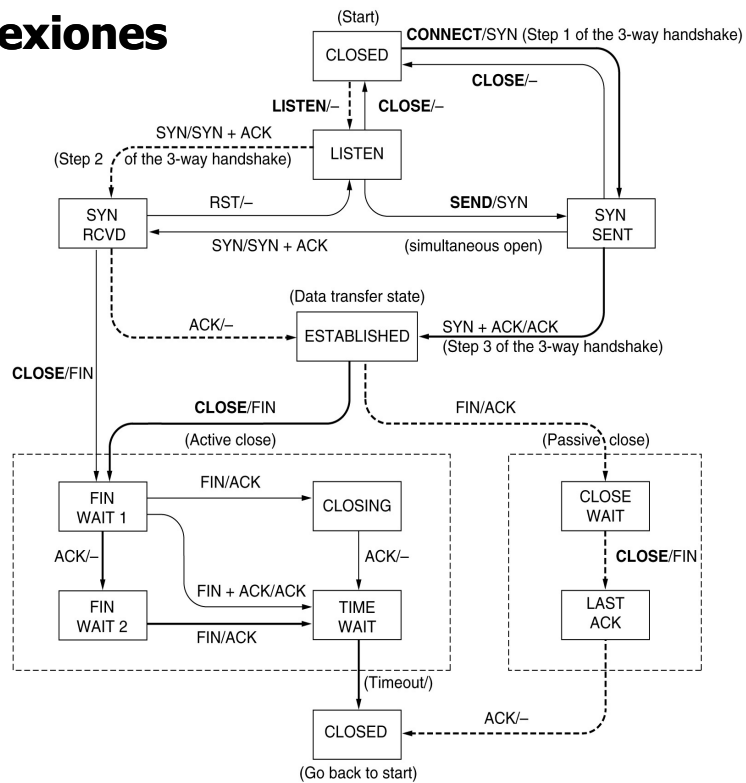
# El protocolo TCP



## Gestión de conexiones

*Línea continua*  
Secuencia normal de estados para el cliente.

*Línea discontinua*  
Secuencia normal de estados para el servidor.

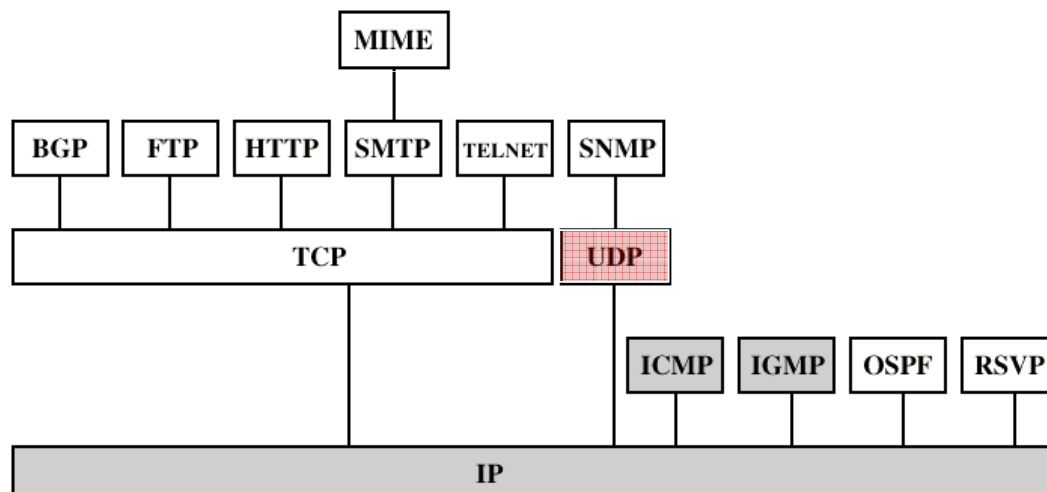


# El protocolo UDP



## User Datagram Protocol

RFC 768: Servicios no orientados a conexión



# El protocolo UDP



## User Datagram Protocol

RFC 768: Servicios no orientados a conexión

### Ventajas:

- Overhead reducido.

### Desventajas:

- Servicio no fiable.
- No se garantiza la entrega.
- No se garantiza la no existencia de duplicados.



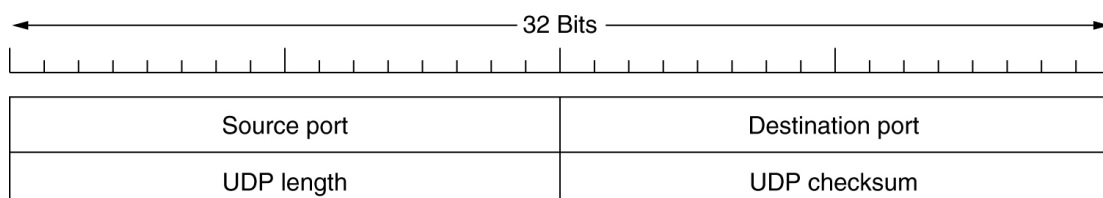
# El protocolo UDP



## User Datagram Protocol

RFC 768: Servicios no orientados a conexión

### Cabecera UDP:



### Usos:

- SNMP [Simple Network Management Protocol]
- RTP [Real-time Transport Protocol]

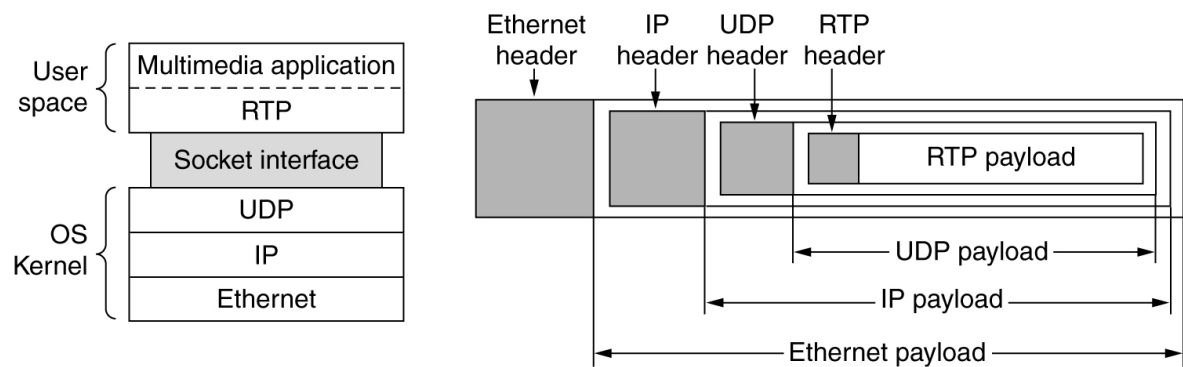


# El protocolo UDP



## Protocolo RTP

### [Real-time Transport Protocol]



# Bibliografía



- Jesús E. Díaz Verdejo; Juan Manuel López Soler & Pedro García Teodoro: **Transmisión de datos y redes de computadores.** Prentice-Hall, 2003. ISBN 84-205-3919-8.
- Douglas E. Comer: **Computer networks and Internets.** Prentice-Hall, 2008 [5ª edición]. ISBN 0-13-606127-3.
- William Stallings: **Comunicaciones y redes de computadores.** Prentice-Hall, 2004 [7ª edición]. ISBN 84-205-4110-9.
- Andrew S. Tanenbaum: **Redes de computadoras.** Prentice-Hall, 2003 [4ª edición]. ISBN 970-260-162-2.

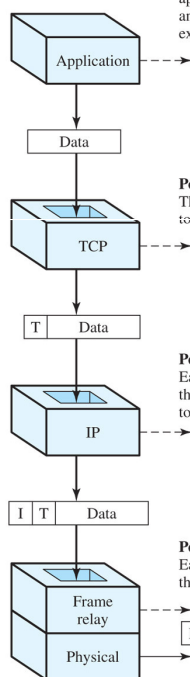




# Apéndice En el emisor



- 1. Preparing the data.** The application protocol prepares a block of data for transmission. For example, an email message (SMTP), a file (FTP), or a block of user input (TELNET).
- 2. Using a common syntax.** If necessary, the data are converted to a form expected by the destination. This may include a different character code, the use of encryption, and/or compression.
- 3. Segmenting the data.** TCP may break the data block into a number of segments, keeping track of their sequence. Each TCP segment includes a header containing a sequence number and a frame check sequence to detect errors.
- 4. Duplicating segments.** A copy is made of each TCP segment, in case the loss or damage of a segment necessitates retransmission. When an acknowledgment is received from the other TCP entity, a segment is erased.
- 5. Fragmenting the segments.** IP may break a TCP segment into a number of datagrams to meet size requirements of the intervening networks. Each datagram includes a header containing a destination address, a frame check sequence, and other control information.
- 6. Framing.** A frame relay header and trailer is added to each IP datagram. The header contains a connection identifier and the trailer contains a frame check sequence.



**Peer-to-peer dialogue.**  
Before data are sent, the sending and receiving applications agree on format and encoding and agree to exchange data.

**Peer-to-peer dialogue.**  
The two TCP entities agree to open a connection.

**Peer-to-peer dialogue.**  
Each IP datagram is forwarded through networks and routers to the destination system.

**Peer-to-peer dialogue.**  
Each frame is forwarded through the frame relay network.

**7. Transmission.** Each frame is transmitted over the medium as a sequence of bits.



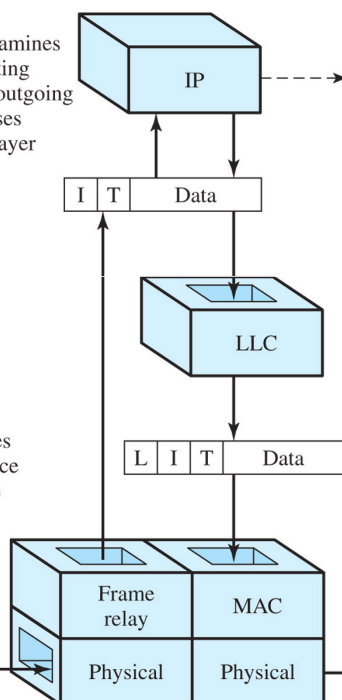
# Apéndice En el router



**10. Routing the packet.** IP examines the IP header and makes a routing decision. It determines which outgoing link is to be used and then passes the datagram back to the link layer for transmission on that link.

**9. Processing the frame.** The frame relay layer removes the header and trailer and processes them. The frame check sequence is used for error detection. The connection number identifies the source.

**8. Arriving at router.** The incoming signal is received over the transmission medium and interpreted as a frame of bits.



**Peer-to-peer dialogue.**  
The router will pass this datagram onto another router or to the destination system.

**11. Forming LLC PDU.** An LLC header is added to each IP datagram to form an LLC PDU. The header contains sequence number and address information.

**12. Framing.** A MAC header and trailer is added to each LLC PDU, forming a MAC frame. The header contains address information and the trailer contains a frame check sequence.

**13. Transmission.** Each frame is transmitted over the medium as a sequence of bits.



# Apéndice En el receptor



**20. Delivering the data.** The application performs any needed transformations, including decompression and decryption, and directs the data to the appropriate file or other destination.

**19. Reassembling user data.** If TCP has broken the user data into multiple segments, these are reassembled and the block is passed up to the application.

**18. Processing the TCP segment.** TCP removes the header. It checks the frame check sequence and acknowledges if there is a match and discards for mismatch. Flow control is also performed.

**17. Processing the IP datagram.** IP removes the header. The frame check sequence and other control information are processed.

**16. Processing the LLC PDU.** The LLC layer removes the header and processes it. The sequence number is used for flow and error control.

**15. Processing the frame.** The MAC layer removes the header and trailer and processes them. The frame check sequence is used for error detection.

**14. Arriving at destination.** The incoming signal is received over the transmission medium and interpreted as a frame of bits.

