

# IDENTIFICACIÓN DE SERVICIOS

## ¿Qué es una red?

Una **red** es un conjunto de ordenadores interconectados entre sí, ya sea mediante cableado o por otros medios inalámbricos.

Actualmente, el desarrollo de tecnologías inalámbricas y de satélite, permiten que las redes de ordenadores tengan un alcance que abarca prácticamente todo el planeta.

## • Tipos de redes

Según el medio de transmisión utilizado



Redes con cables  
Inalámbricas

Según la zona



geográfica que abarcan

LAN (Locales)  
MAN (Metropolitanas)  
WAN (Extendidas)

Según el sistema de red utilizado



Cliente-Servidor  
Punto a punto

Según la propiedad de las líneas



Públicas  
Privadas

## Redes según el medio de transmisión utilizado

### Redes con cables

La información viaja a través de un soporte físico concreto como el cable (medios de transmisión guiados).

### Redes inalámbricas

Utilizan medios de transmisión no guiados (sin cables) para la comunicación de datos entre emisor y receptor.

## • Redes según la zona geográfica que abarcan

### Redes de área local

Las LAN (Local Área Network) son redes que abarcan una zona reducida. Generalmente constan de varios ordenadores localizados en el mismo edificio, interconectados mediante cables o por medios inalámbricos.

#### Tecnologías utilizadas:

Entre las tecnologías con cables están Ethernet, Fast Ethernet, Gigabit Ethernet.

Con redes inalámbricas la tecnología más usual es Wifi (Wireless-Fidelity).

**¿Quién las utiliza?** Las redes locales se utilizan en entornos como empresas o entidades oficiales, aunque también las emplean los profesionales autónomos y empiezan a ser habituales en el ámbito doméstico (mini redes).

### Redes de área metropolitana

Las MAN (Metropolitan Área Network) suelen ser redes de área local interconectadas, es decir, redes de redes. Abarcan una zona geográfica mayor que las LAN (por ejemplo, una ciudad o un grupo de oficinas cercanas) y su capacidad de transmisión también es mayor.

### Redes de área extendida

Las WAN (Wide Área Network), o redes de gran alcance, abarcan una región más extensa que puede variar entre unos kilómetros y distancias continentales. En ellas los enlaces se establecen generalmente por medio de líneas telefónicas o líneas de alta velocidad; por ejemplo, líneas de fibra óptica o satélites.

## • Redes según el sistema de red utilizado

### Redes cliente-servidor

Se trata de redes utilizadas en las empresas, en las que uno o varios ordenadores (servidores) proporcionan servicios a otros (clientes). Los servidores son manejados por el administrador de red. Este sistema está diseñado para controlar grandes volúmenes de tráfico en la red y proporcionar servicios complejos como archivos, impresión, comunicaciones, correo electrónico, Web, etc.

### Redes punto a punto

En su estructura, todos los ordenadores tienen las mismas prestaciones y son sus usuarios quienes deciden qué información desean compartir y con quién. Cualquier PC del grupo puede hacer de servidor (por ejemplo, compartiendo sus archivos), de cliente (como cuando se utiliza la impresora de otro), o ambas funciones a la vez. La más pequeña está formada por dos dispositivos.

## • Redes Según la propiedad de las líneas

### Redes privadas

Todo el recorrido de las líneas utilizadas en la red es propiedad de la empresa que la posee.

### Redes públicas

En este caso, las líneas de la red son de titularidad pública (compañías telefónicas generalmente); por tanto, su ámbito de actuación es nacional o transnacional. La empresa privada utiliza las líneas en régimen de alquiler.

## • **Medios de transmisión inalámbricos**

### **Microondas**

Terrestres o por satélite. En las terrestres se utilizan antenas parabólicas situadas en lugares altos y se consiguen transmisiones que alcanzan entre 50 y 100 kilómetros. En el caso de los satélites artificiales, se logran transmisiones de gran capacidad mediante una estación situada en el espacio que se utiliza como enlace entre dos o más estaciones terrestres que emiten y transmiten.

### **Ondas de radio**

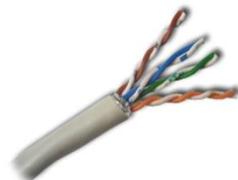
Los equipos llevan incorporado un pequeño transmisor/receptor de radio que recoge los datos y los envía a otros ordenadores de la red. Disponen de baja capacidad de transmisión en comparación con una conexión con cables. Wifi y bluetooth son sistemas que utilizan las ondas de radio para la transmisión de los datos en los campos de telecomunicaciones e informática.

### **Ondas de infrarrojos**

Este sistema consiste en instalar emisores/receptores de infrarrojos en distancias cortas y sin obstáculos en su trayecto. Tienen el inconveniente de presentar gran sensibilidad a las interferencias y se utilizan en redes locales de ámbito pequeño.

## • Tipos de cable

### El par trenzado



Está formado por pares de conductores aislados trenzados entre sí. La forma trenzada se utiliza para reducir la interferencia eléctrica de pares cercanos o dentro de su envoltura. Existen dos tipos: STP (apantallado: recubierto de una malla metálica) y UTP (no apantallado). Un cable de par trenzado tiene en sus extremos conectores RJ-45, en los que los hilos deben llevar un orden determinado.

### El cable coaxial

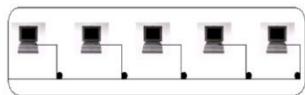


Es menos susceptible a interferencias que el cable de par trenzado, se puede utilizar para cubrir mayores distancias y es posible conectar más estaciones en una línea compartida.

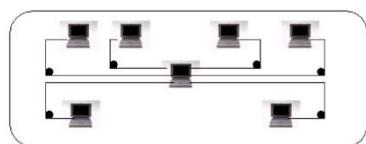
### La fibra óptica

Consiste en un delgadísimo hilo de cristal o plástico a través el cual se transmiten señales luminosas.

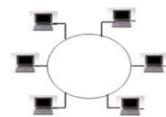
## • Topología de las redes cableadas



BUS



ESTRELLA



ANILLO

- El bus actúa como canal principal donde se enlazan el resto de dispositivos de la red.
  - No existe ningún equipo que controle la red.
  - Este tipo de conexión es muy sencilla y tiene un bajo coste.
  - Principal inconveniente: un fallo del bus repercute en todos los dispositivos de la red.
- 
- Todos los equipos van conectados a un dispositivo central (hub o conmutador) que se encarga de realizar todo el intercambio de información entre todos los ordenadores.
  - El concentrador aisla a la red de los problemas que puedan surgir en uno de los equipos.
  - Inconveniente: mucho gasto en cableado.
- 
- El anillo es un bus cerrado en sus extremos.
  - La red en anillo más extendida está diseñada por IBM y se denomina *Token Ring*.
  - Los equipos se conectan a un concentrador especializado.
  - Los bits se transmiten de un ordenador a otro en un solo sentido, por lo que si existe una mala conexión en uno de los equipos se traduce en una disminución considerable del rendimiento general de la red.

- **Componentes de una red local**

- Tarjetas de red
- Cableado
- Medios de transmisión inalámbricos
- Estaciones de trabajo
- Servidor
- Dispositivos distribuidores
- Puntos de acceso
- Recursos compartidos
- Sistema operativo específico

# Modelos de Comunicación

- Para que esto suceda, los dos equipos deben saber, por adelantado, cómo se espera que se comuniquen.
- ¿Cómo inician la conversación?
- ¿A quién le toca comunicarse?
- ¿Cómo sabe un equipo si su mensaje se ha transmitido correctamente?
- ¿Cómo terminan la conversación?

# Modelos de Referencia

- Modelo OSI
- Modelo TCPIP

# **MODELOS OSI Y TCP/IP EN LAS REDES DE DATOS**

## **Modelo de capas y protocolos de comunicaciones.**

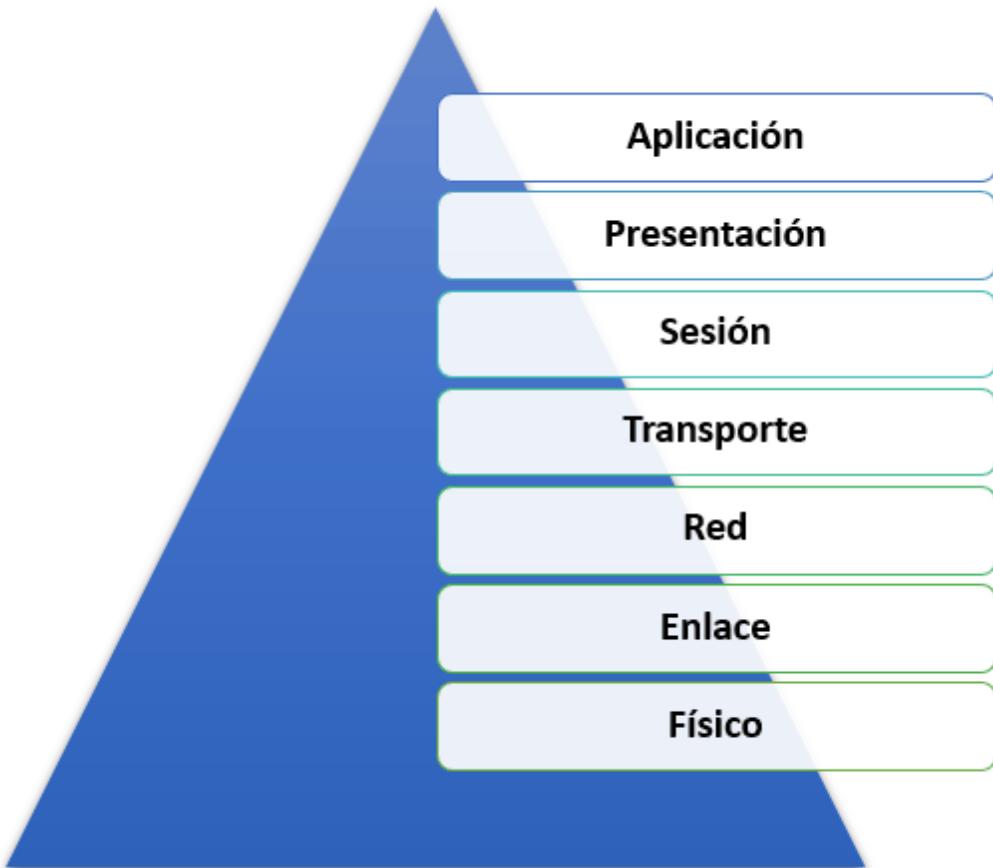
### **El modelo de referencia OSI:**

- Es una normativa de la Organización Internacional de Normalización (**ISO**).
- Es una arquitectura de red estándar, compuesta por **7** capas.
- Tiene como objetivo establecer un marco de referencia para la definición de arquitecturas en la interconexión de los sistemas de comunicaciones.

### **El modelo de referencia TCP/IP:**

- También llamado *Modelo de Internet*.
- Es el utilizado en la práctica para describir arquitecturas de red en Internet.
- Ha sido estandarizado por el organismo **IETF**(*Internet Engineering Task Force*).
- En este caso la arquitectura de red está compuesta por **4** capas.

# Modelo OSI



## LA PILA OSI

### Nivel de Aplicación

Servicios de red a aplicaciones

### Nivel de Presentación

Representación de los datos

### Nivel de Sesión

Comunicación entre dispositivos de la red

### Nivel de Transporte

Conexión extremo-a-extremo y fiabilidad de los datos

### Nivel de Red

Determinación de ruta e IP (Direccionamiento lógico)

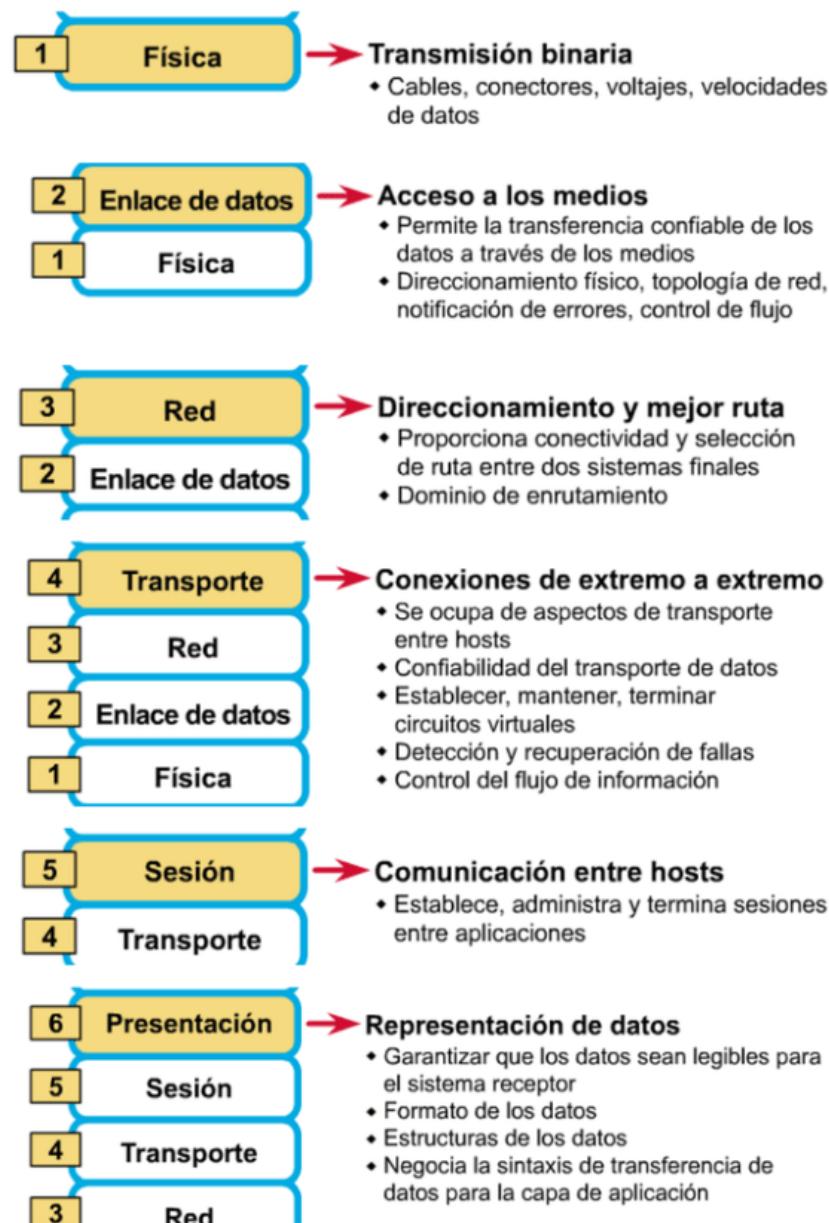
### Nivel de Enlace de Datos

Direccionamiento físico (MAC y LLC)

### Nivel Físico

Señal y transmisión binaria

## MODELO OSI Y DISPOSITIVOS DE RED POR CAPA



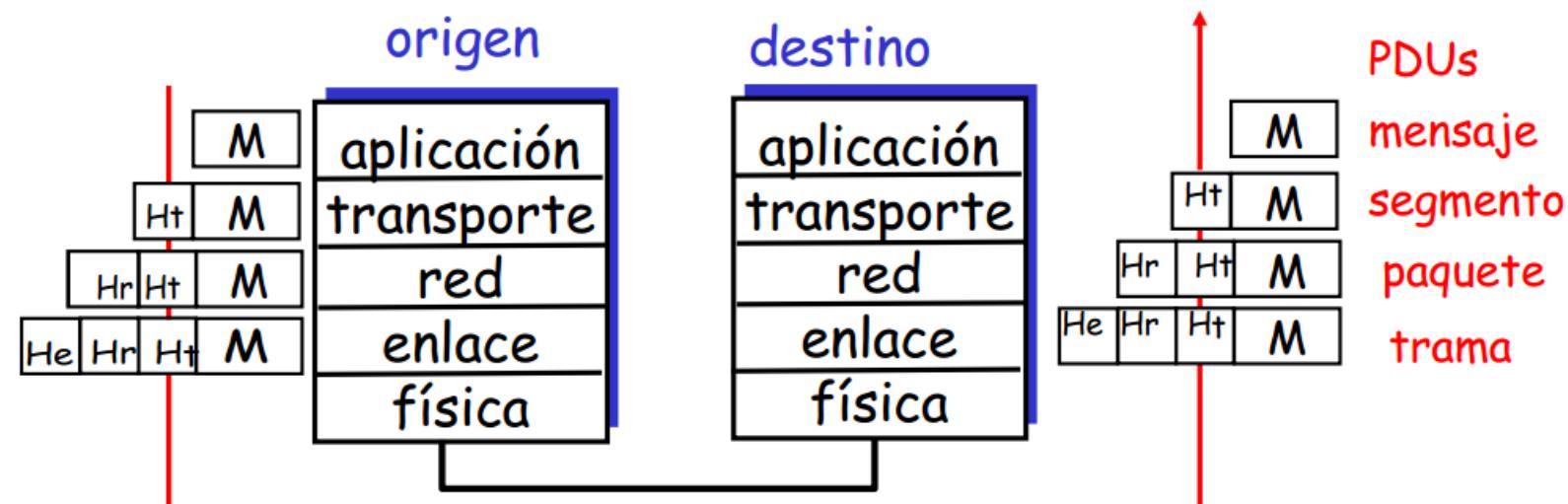
# MODELOS OSI Y TCP/IP EN LAS REDES DE DATOS

Modelo de capas y protocolos de comunicaciones.

Capas de los protocolos y los datos

Cada capa toma los datos de la capa superior:

- Agrega información de control (cabecera) y crea una nueva unidad de datos (PDU)
- Pasa esta nueva unidad de datos a la capa inferior.



# MODELOS OSI Y TCP/IP EN LAS REDES DE DATOS

## Modelo de capas y protocolos de comunicaciones.

### PROCESO DE ENVÍO Y RECEPCIÓN

Cuando se envían mensajes en una red, el stack del protocolo de un host funciona desde arriba hacia abajo, en un primer momento.

Posteriormente, el host receptor realiza la operación inversa, siguiendo el orden de abajo arriba.

Tomando como base el modelo TCP/IP, la secuencia de eventos sería la siguiente:

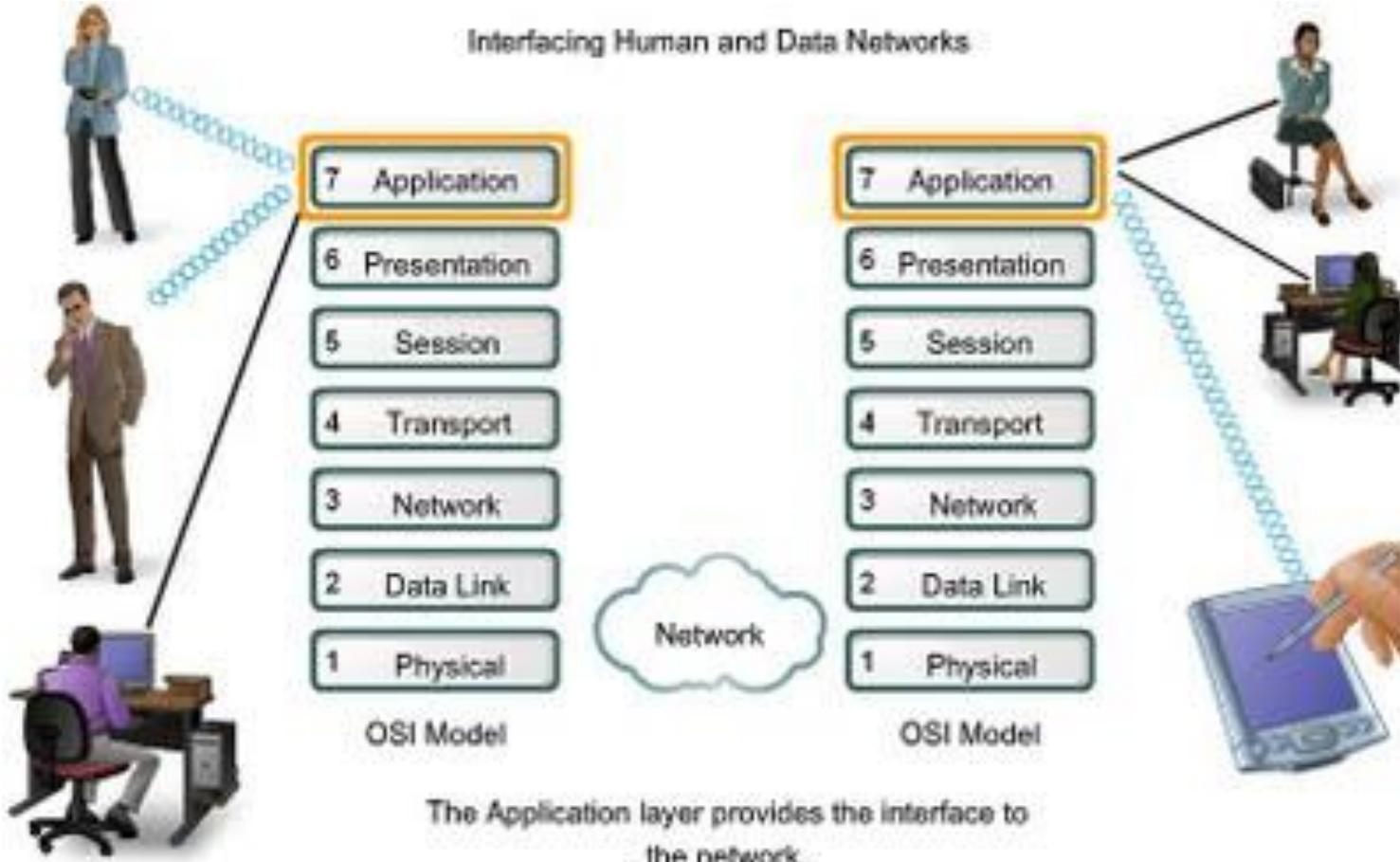
1. Los **datos** son encapsulados en **segmentos**.
2. Los **segmentos** se encapsulan en **paquetes**.
3. Los **paquetes** se convierten en **tramas**.
4. Las **tramas** son transmitidas en forma de **bits**.

**EMISOR**  
Encapsulación

1. Los **bits** se convierten en **tramas**.
2. Las **tramas** se desencapsulan en **paquetes**.
3. Los **paquetes** se desencapsulan en **segmentos**.
4. Los **segmentos** se convierten en **datos** de la capa de aplicación.

**RECEPTOR**  
Desencapsulación

# CAPA APLICACIÓN



# Modelo TCPIP

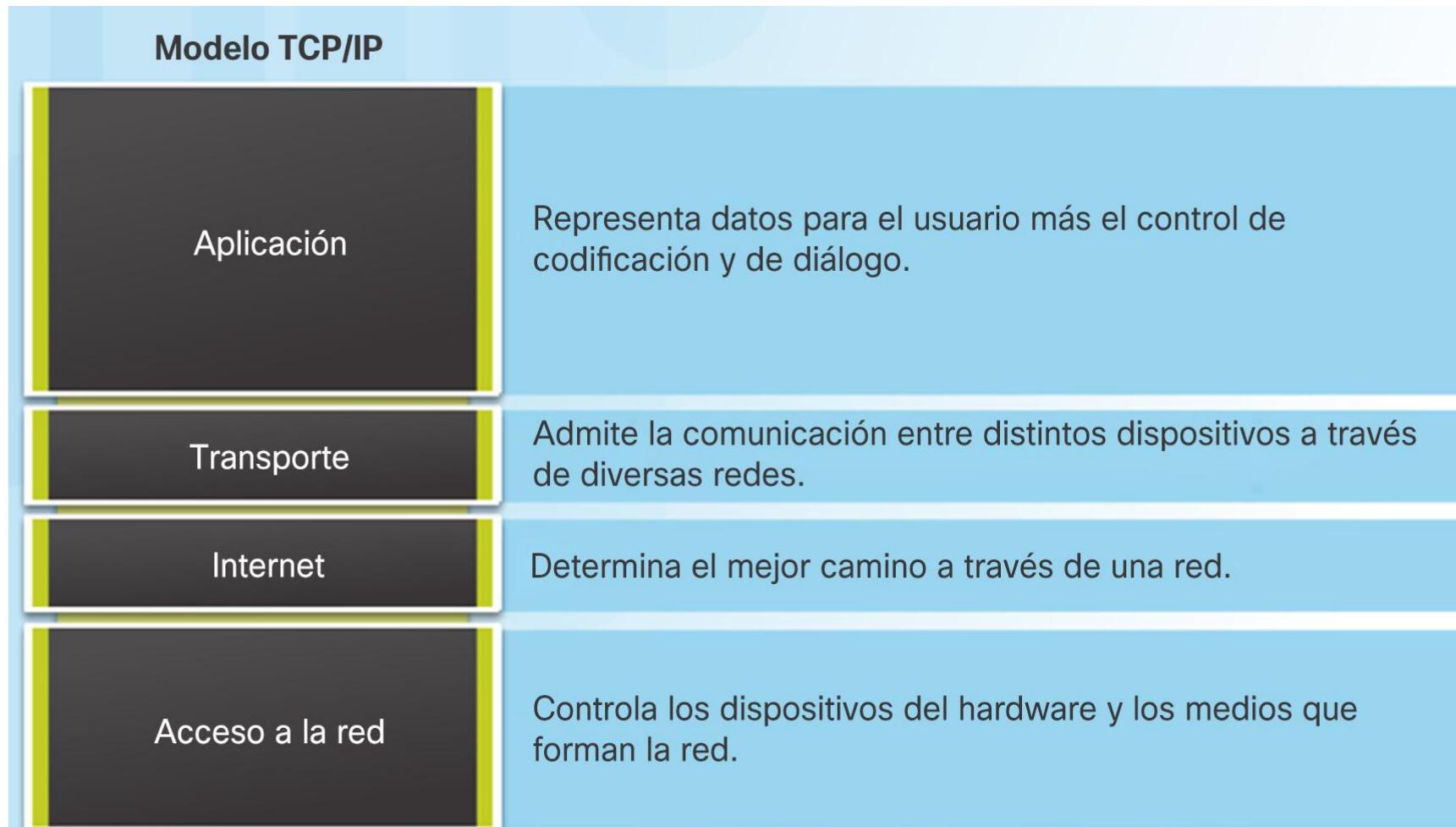
- El modelo TCP/IP es una explicación de protocolos de red creado por Vinton Cerf y Robert E. Kahn, en la década de 1970. Fue implantado en la red ARPANET, la primera red de área amplia (WAN), desarrollada por encargo de DARPA, una agencia (Departamento de Defensa de los Estados Unidos) y predecesora de Internet; por esta razón, a veces también se le llama modelo DoD o modelo DARPA.
- El modelo TCP/IP es usado para comunicaciones en redes y, como todo protocolo, describe un conjunto de guías generales de operación para permitir que un equipo pueda comunicarse en una red. TCP/IP provee conectividad de extremo a extremo especificando cómo los datos deberían ser formateados, direccionados, transmitidos, enrutados y recibidos por el destinatario.

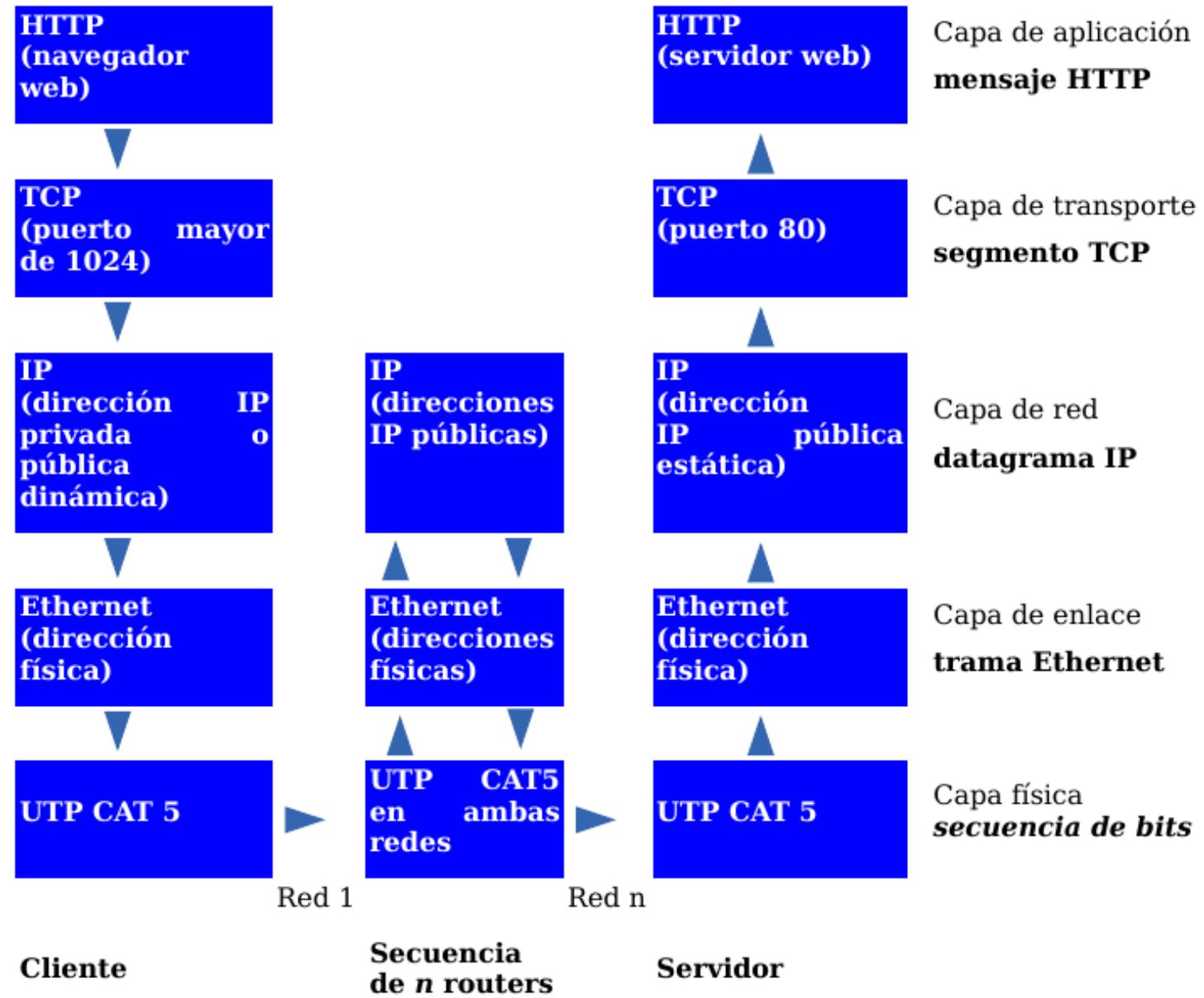
- Para conseguir un intercambio fiable de datos entre dos equipos, se deben llevar a cabo muchos procedimientos separados. El resultado es que el software de comunicaciones es complejo. Con un modelo en capas o niveles resulta más sencillo agrupar funciones relacionadas e implementar el software modular de comunicaciones.
- Las capas están jerarquizadas. Cada capa se construye sobre su predecesora. El número de capas y, en cada una de ellas, sus servicios y funciones son variables con cada tipo de red.
- un sistema de protocolos que hacen posibles servicios Telnet, FTP, E-mail, y otros entre ordenadores que no pertenecen a la misma red.

# PROTOCOLO TCP/IP (II)

- El **Protocolo de Control de Transmisión (TCP)** permite a dos anfitriones establecer una conexión e intercambiar datos. El TCP garantiza la entrega de datos, es decir, que los datos no se pierdan durante la transmisión y también garantiza que los paquetes sean entregados en el mismo orden en el cual fueron enviados.
- El **Protocolo de Internet (IP)** utiliza direcciones que son series de cuatro números octetos (byte) con un formato de punto decimal, por ejemplo: 69.5.163.59
- Los Protocolos de Aplicación como HTTP y FTP se basan y utilizan TCP/IP.

# Modelo TCP/IP





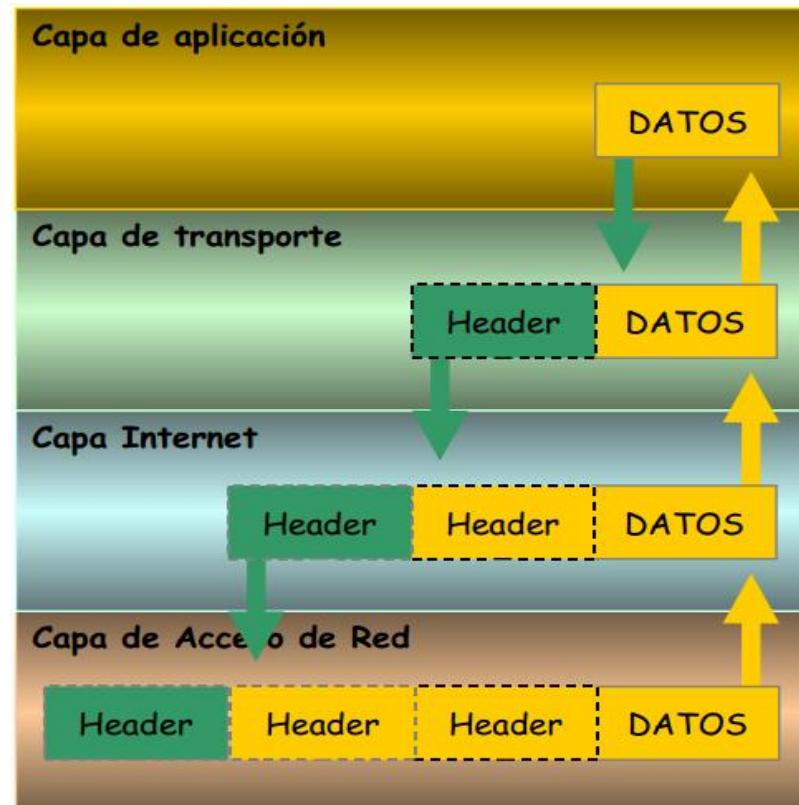
# MODELOS OSI Y TCP/IP EN LAS REDES DE DATOS

## Modelo de capas y protocolos de comunicaciones.

### Encapsulación de datos

Cada capa de la pila TCP/IP agrega información de control (cabeceras) para asegurar la entrega correcta de los datos.

Cuando se recibe, la información de control se retira una vez sea utilizada.



# CAPA Aplicación

- La capa de aplicación incluye los protocolos utilizados por la mayoría de las aplicaciones para proporcionar servicios de usuario o intercambiar datos de aplicaciones a través de las conexiones de red establecidas por los protocolos de las capas inferiores.
- Ejemplos: protocolo HTTP o Protocolo de Transferencia de Hipertexto, el protocolo FTP o Protocolo de Transferencia de Archivos, el protocolo SMTP o protocolo de Transferencia de Correo y el Protocolo DHCP o Protocolo de Configuración Dinámica de Host.

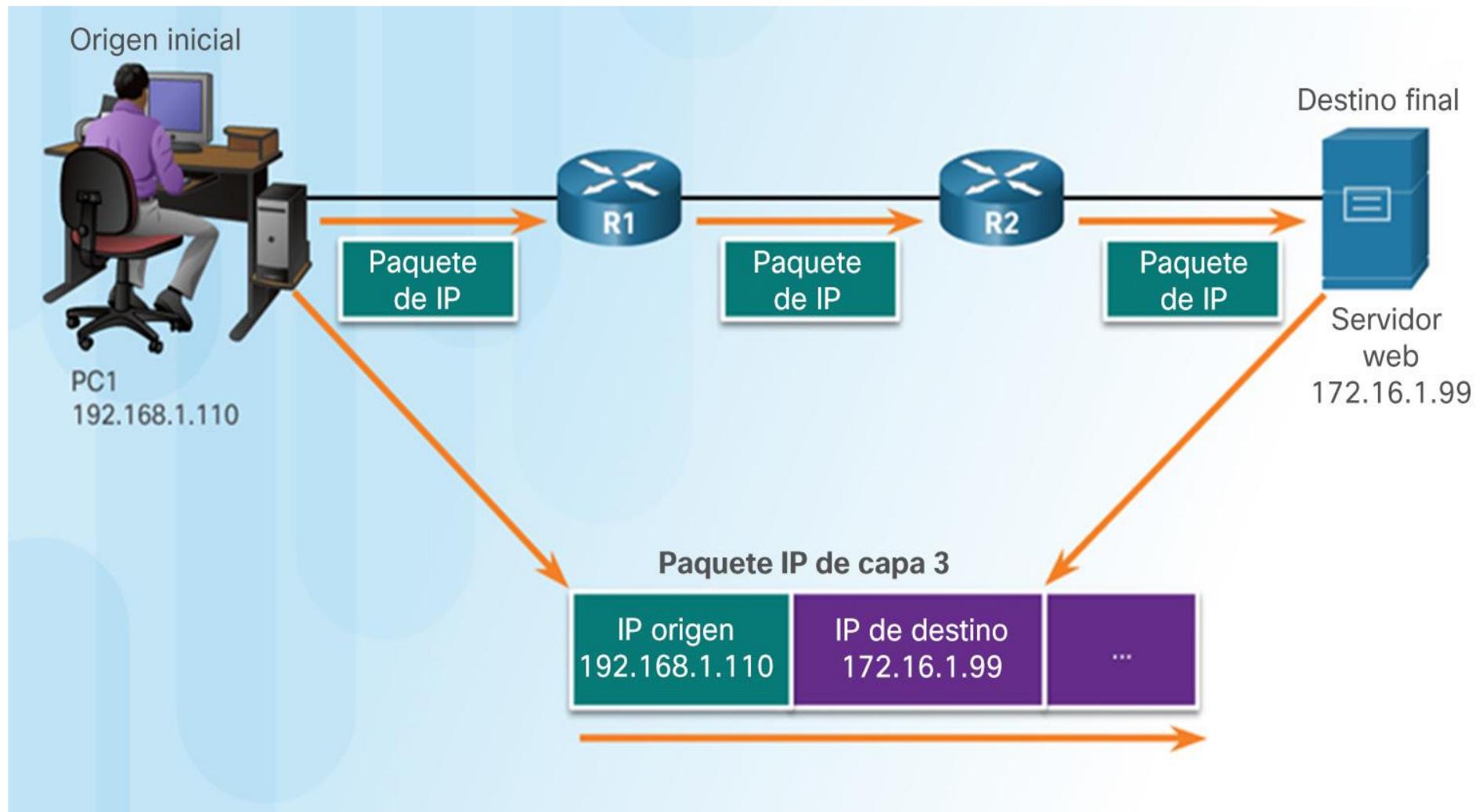
# CAPA Transporte

- se establecen canales de datos básicos utilizadas para hacer posible el intercambio de datos. Además establece la conectividad de host a host en forma de servicios de transferencia de mensajes de extremo a extremo independientes de las redes subyacentes e independientes de la estructura de los datos del usuario y la logística del intercambio de información.
- La capa de transporte tiene 2 tipos de conexiones y son orientada a la conexión como es el TCP, o no orientado a la conexión como es el UDP. Los protocolos de esta capa pueden proporcionar control de errores, segmentación, control de flujo, control de congestión y direccionamiento de aplicaciones.

# CAPA internet

- IP
  - Es un número que identifica, de manera lógica y jerárquica, a una Interfaz en red (elemento de comunicación/conexión) de un dispositivo
- ICMP
  - **protocolo de control de mensajes de Internet** (en inglés: **Internet Control Message Protocol** y conocido por sus siglas **ICMP**) es parte del conjunto de protocolos IP. Es utilizado para enviar mensajes de error e información operativa indicando, por ejemplo, que un host no puede ser localizado o que un servicio que se ha solicitado no está disponible. Estos mensajes del protocolo ICMP se envían a la dirección IP de origen del paquete.

- Direcciones IP origen y destino



# Clase de Direcciones IP

- 

Clase	Bits iniciales	Intervalo (*)	N.º de redes	N.º de direcciones por red	N.º de hosts por red(†)	Máscara de red	Dirección de broadcast
A	0	0.0.0.0 (**)- 127.255.255.255 (†)	128	16 777 216	16 777 214	255.0.0.0	x.255.255.255
B	10	128.0.0.0 - 191.255.255.255	16 382	65 536	65 534	255.255.0.0	x.x.255.255
C	110	192.0.0.0 - 223.255.255.255	2 097 150	256	254	255.255.255.0	x.x.x.255
D (Multicast)	1110	224.0.0.0 - 239.255.255.255					
E (experimental)	1111	240.0.0.0 - 255.255.255.254					

# EJERCICIO

- IP ¿Cómo se calcula?
- ¿Cómo sabemos que 2 equipos están en la misma red?
- ¿cuál es la puerta de enlace?
- ¿Cómo se asigna una IP?¿Quién lo hace?

# CAPA RED

- Nos proporciona el direccionamiento físico. Su MAC ....

# MAC, ¿Eso qué es?

- ¿Qué es?
- ¿Es única para cada equipo?
- ¿Cómo se asigna?

# EQUIVALENCIAS

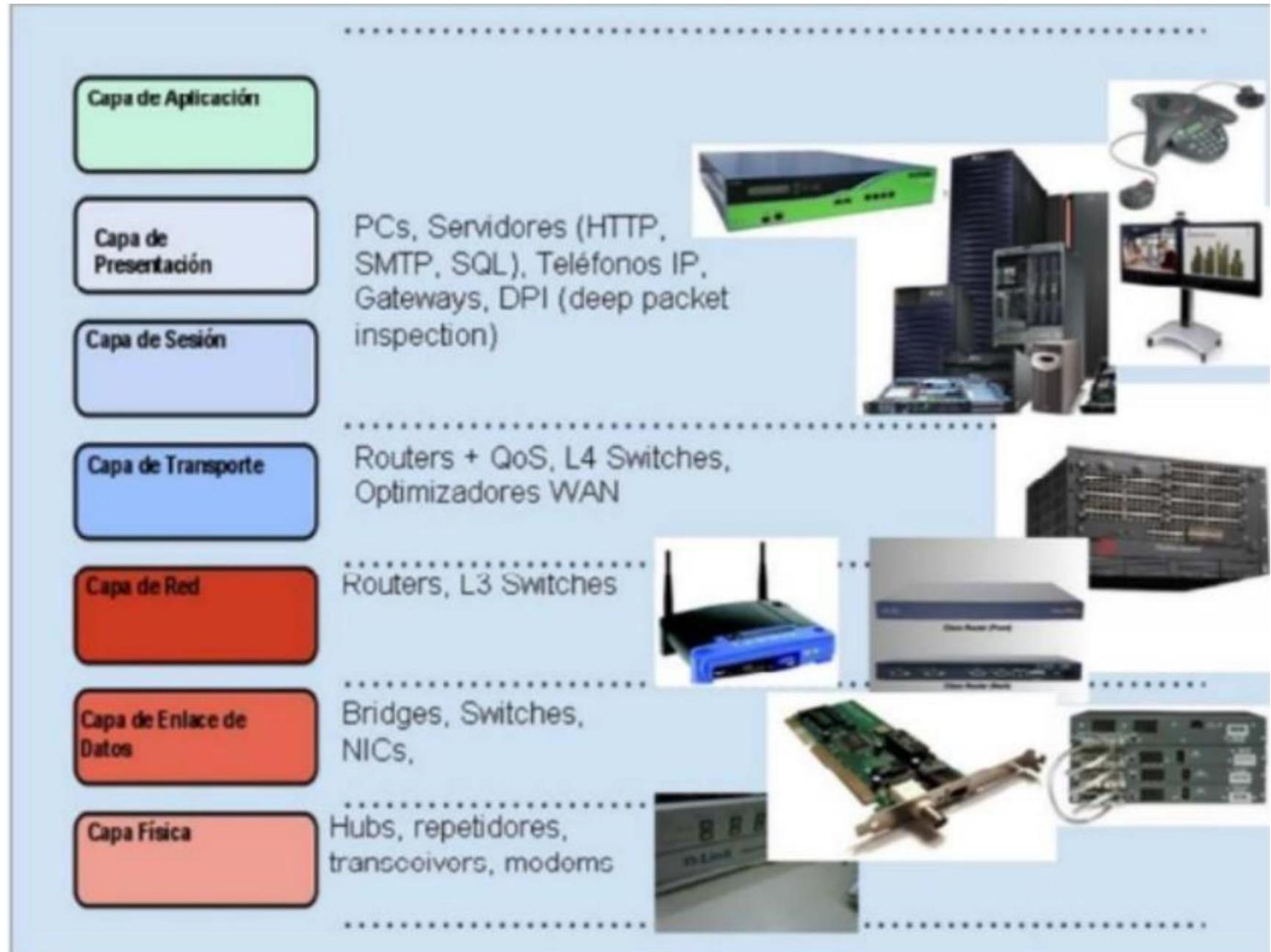
## LA PILA OSI

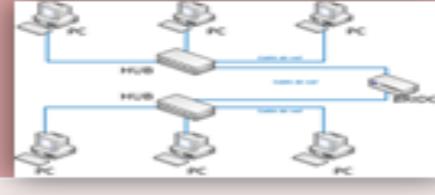


## • Asociaciones de estándares

<b>ETSI</b>	Instituto Europeo de Estándares de Telecomunicaciones.
<b>ANSI</b>	Instituto Nacional de Estándares Americano.
<b>IEEE</b>	Instituto de Ingeniería Eléctrica y Electrónica.
<b>ISO</b>	Organismo Internacional de Estandarización.
<b>TIA</b>	Asociación de la Industria de las Telecomunicaciones.

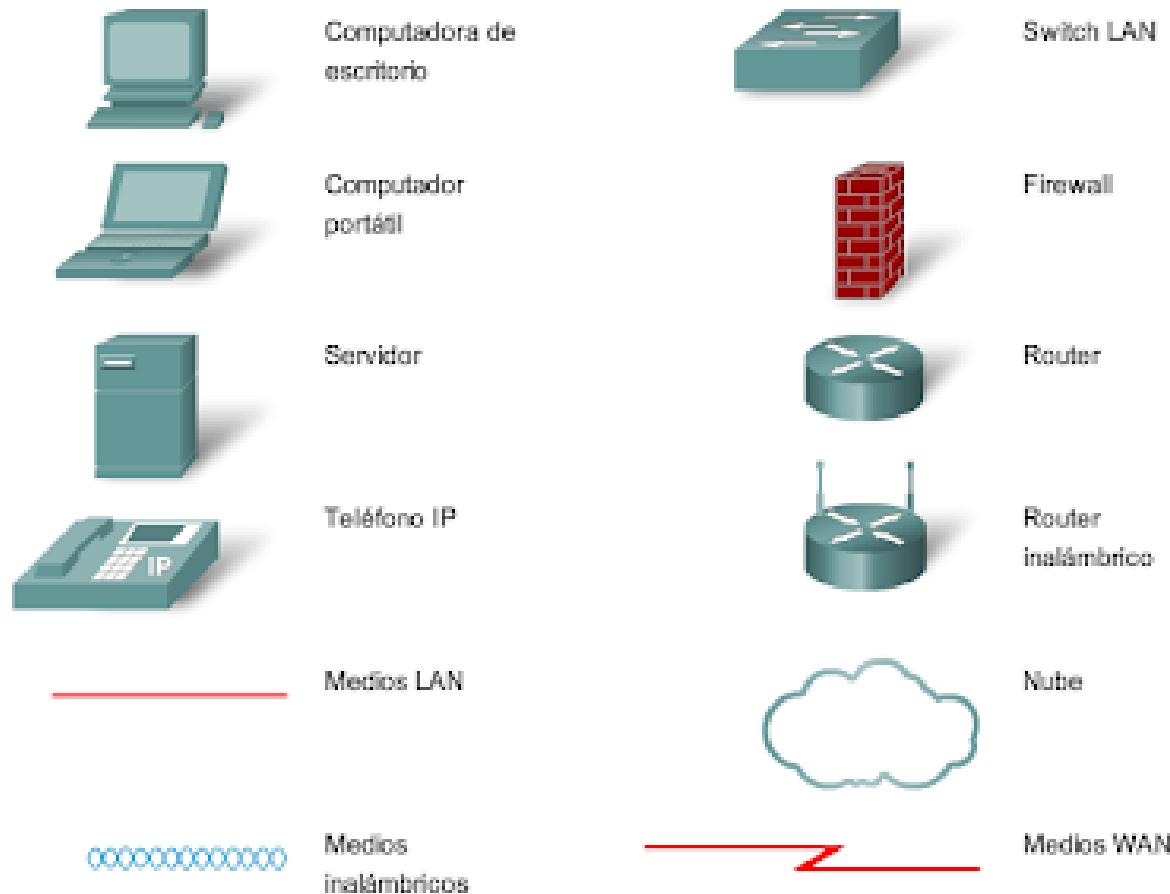
# Elementos por capa



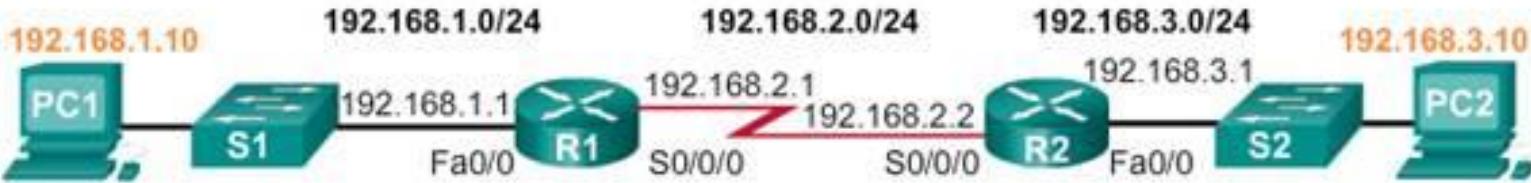
<b>Hardware</b>	<b>Uso</b>	<b>Lo que ocasiona cuando falla.</b>	<b>Imagen</b>
Modem	Convierte señales digitales en analógicas y permite la conexión a internet vía las líneas telefónicas.	Se interrumpe la conexión a internet.	
Gateway	Interconecta las redes por medio de protocolos.	Se interrumpe la conexión en la red.	
Hub	Centraliza el cableado y lo amplia.	Disminuye la señal y corta su conexión.	
Switch	Interconexión de equipos que opera la capa enlace de datos.	Se interrumpe la conexión entre los dispositivos.	
Bridge	Interconecta las redes de ordenación que opera la capa de enlace de datos.	Se interrumpen las redes que están conectadas.	
Router	Proporciona conectividad a nivel de red.	Se interrumpe la conectividad con la red.	

# Representación gráfica

Simbolos comunes de las redes de datos



## Registro del direccionamiento de red



Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
R1	Fa0/0	192.168.1.1	255.255.255.0	N/A
	S0/0/0	192.168.2.1	255.255.255.0	N/A
R2	Fa0/0	192.168.3.1	255.255.255.0	N/A
	S0/0/0	192.168.2.2	255.255.255.0	N/A
PC1	N/A	192.168.1.10	255.255.255.0	192.168.1.1
PC2	N/A	192.168.3.10	255.255.255.0	192.168.3.1

## • Comprobar el funcionamiento de la red

Orden PING	Con esta orden se consigue saber si la conexión con el otro equipo es posible.
Orden IPCONFIG	Se utiliza para averiguar la dirección IP de cualquier adaptador de red
Utilidad NETSTAT	Proporciona información sobre el estado de la red.
monitor de recursos	Permite recopilar información sobre el tráfico de red del equipo central con los clientes y viceversa.
Comando NSLOOKUP	Sirve para obtener las direcciones IP a partir de nombres DNS.

# EJERCICIO

- Ver qué hacen los comandos:
  - PING, TRACERT, NETSTAT, tcpdump, ifconfig
  - ¿Son iguales en Windows /Linux?
  - Poner ambos nombres y explicar qué hacen.

## • Intranet y Extranet

### INTRANET

Es una red de comunicaciones idéntica a Internet, pero su uso está limitado a un entorno concreto, definido y limitado. Se trata de redes privadas empresariales o educativas que emplea los protocolos de Internet para el transporte de datos; esto permite a las empresas que disponen de ella, que sus empleados tengan acceso y uso compartido y simultáneo de información y recursos. Sin embargo, desde la red Internet un usuario cualquiera no puede acceder a la Intranet, ya que tiene acceso restringido.

### EXTRANET

Es una red orientada a personas ajenas a la empresa, que ha surgido de la ampliación de las Intranets. La Extranet conecta a la empresa con sus socios, clientes, proveedores... y establece diferentes niveles de acceso a la información.

## • Procedimientos de protección de datos

<b>Firewall de Windows</b>	Ayuda a proteger el equipo al impedir que usuarios sin autorización puedan acceder a la información a través de Internet.
<b>Windows Defender</b>	Se trata de un software que incluye Windows y se ejecuta automáticamente cuando se activa. Ayuda a proteger el equipo de spyware.
<b>Antivirus</b>	Aunque la mayor parte de los cortafuegos (Firewall) evita que los virus y gusanos lleguen a nuestro equipo, no los detecta ni los deshabilita si ya se encuentran instalados. Esta última labor la realizan los antivirus.
<b>Centro de actividades</b>	El Centro de actividades avisa de que el firewall está activado, de que el antivirus está actualizado y de que las actualizaciones se instalan automáticamente.
<b>Control de cuentas de usuario</b>	Es una característica predeterminada de Windows que avisa antes de realizar cambios en el equipo que requieren permisos de administrador.
<b>Copias de seguridad</b>	Cada cierto tiempo, conviene guardar todos los datos importantes, sobre todo si se trata de documentación de la empresa.

<b>Eliminación de los datos privados</b>	Al utilizar un navegador en la conexión a Internet, quedan almacenados datos privados al término de la conexión. Por seguridad, es aconsejable configurar el navegador para que los elimine automáticamente
<b>Empleo de contraseñas seguras</b>	Una contraseña es segura cuando es difícil de adivinar.
<b>Navegadores con protección alta</b>	Permiten salvaguardar ciertos datos.
<b>Programas y servidores de correo electrónico blindados</b>	Todos incorporan opciones de seguridad. Por ejemplo, Gmail posee una potente tecnología para bloquear virus y gusanos, filtrar correo no deseado y avisar cuando se reciben mensajes con identidad suplantada (phishing).

# ¿QUÉ ES UN PROTOCOLO?

- es un protocolo de comunicación de datos digitales clasificado funcionalmente en la capa de red según el modelo internacional OSI.
- Su función principal es el uso bidireccional en origen o destino de comunicación para transmitir datos mediante un protocolo no orientado a conexión que transfiere paquetes conmutados a través de distintas redes físicas previamente enlazadas según la norma OSI de enlace de datos.

- **Protocolos de comunicación**

<b>NetBEUI</b>	Interfaz extendida de usuario de NetBIOS. Desarrollado originalmente para redes IBM, fue usado por Microsoft para sus redes por primera vez a mediados de la década de 1980. Ha sido el protocolo por defecto de Microsoft. Es pequeño y veloz, necesita poca memoria y ejecuta una óptima comprobación de errores, pero está ajustado para pequeñas redes, por lo que si es utilizado en las grandes su rendimiento es escaso. Además no es direccionable.
<b>TCP/IP</b>	Protocolo de control de transmisión/protocolo Internet. Se suele usar sobre redes de área extendida como Internet y, para comunicarse con ordenadores que ejecutan alguna versión del sistema operativo UNIX. Es un conjunto de protocolos y es el más completo y más aceptado del mundo. Aunque tiene reputación de ser difícil de configurar, las nuevas implantaciones lo están haciendo más sencillo. Es direccionable, pero no es tan rápido como NetBEUI en pequeñas redes.
<b>Infrarrojos</b>	Permite conectarse en red con otros ordenadores a través de puertos para infrarrojos.

- **Protocolos de seguridad para redes inalámbricas**

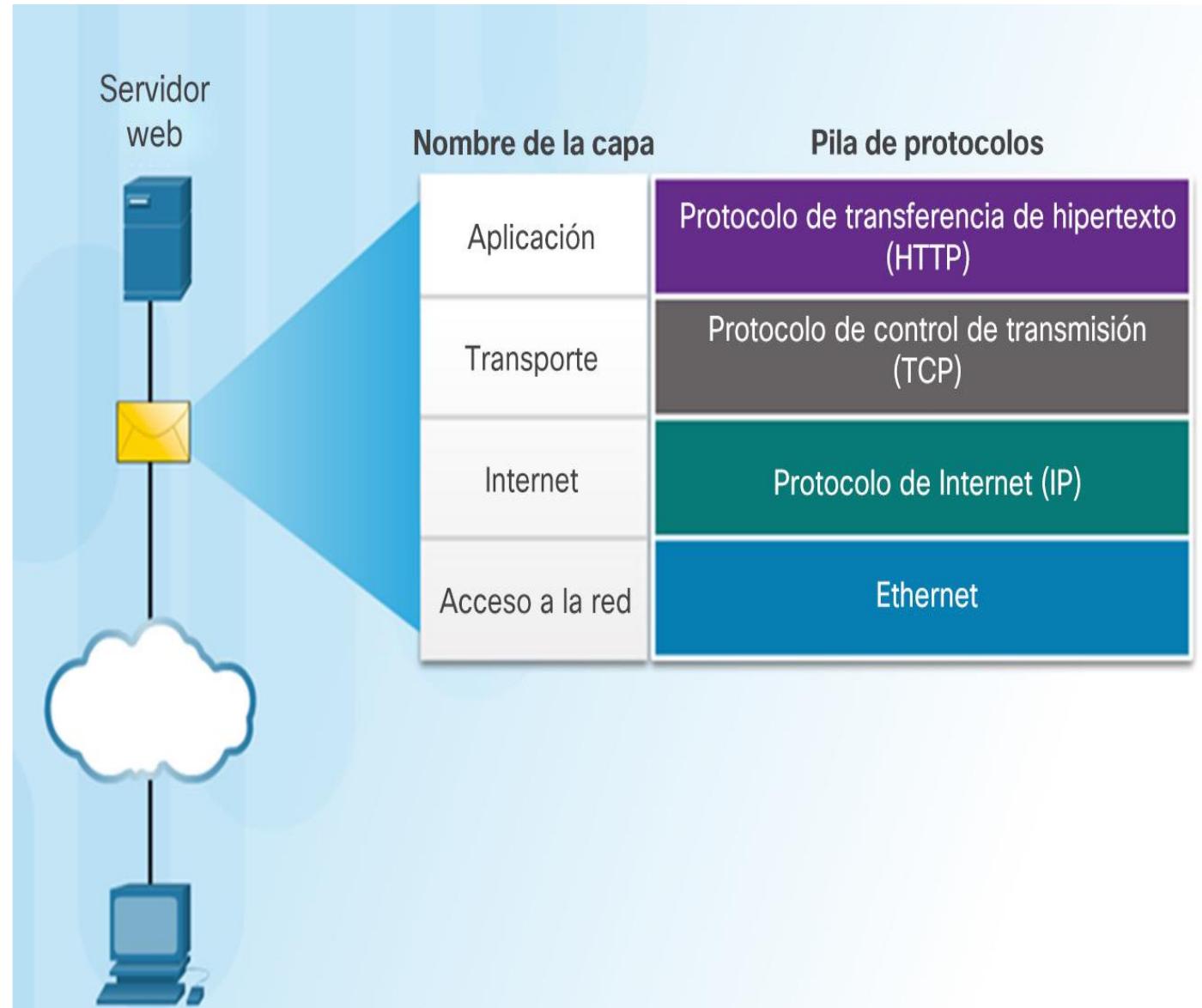
### WEP

**Wired Equivalent Privacy.** Se basa en la encriptación de los datos durante el tiempo que dura su transmisión de un punto a otro de la red. Ofrece el mismo nivel de seguridad que el de las redes LAN cableadas.

### WPA

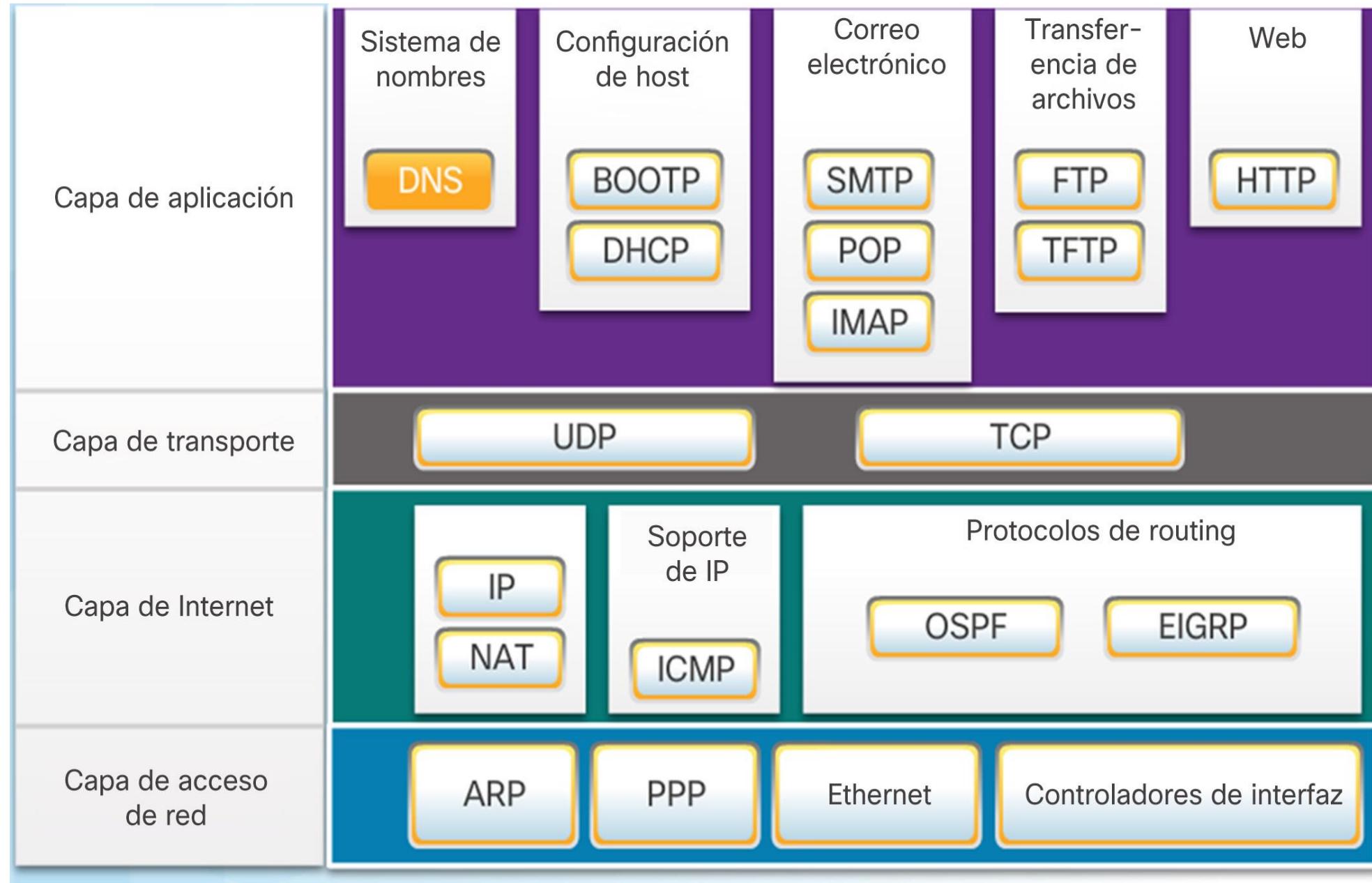
Wi-Fi Protected Access. Surgió para corregir las deficiencias del protocolo WEP. Dentro del WPA se usa el TKIP (Temporal Key Integrity Protocol). No es un protocolo como tal. Protege la información cambiando las claves de acceso cada 10 000 paquetes.

- La comunicación entre un servidor web y un cliente web es un ejemplo de interacción entre varios protocolos:  
**HTTP**: protocolo de aplicación que rige la forma en que interactúan un servidor web y un cliente web.
- **TCP**: protocolo de transporte que administra las conversaciones individuales.
- **IP**: encapsula los segmentos TCP en paquetes, asigna direcciones y entrega al host de destino.
- **Ethernet**: permite la comunicación a través de un enlace de datos y la transmisión física de datos en los medios de r



- Suites de protocolos y estándares de la industria
- Una suite de protocolos es un grupo de protocolos que trabajan en forma conjunta para proporcionar servicios integrales de comunicación de red.

Nombre de la capa	TCP/IP	ISO	AppleTalk	Novell Netware
Aplicación	HTTP DNS DHCP FTP	ACSE ROSE TRSE SESE	AFP	NDS
Transporte	TCP UDP	TP0 TP1 TP2 TP3 TP4	ATP AEP NBP RTMP	SPX
Internet	IPv4 IPv6 ICMPv4 ICMPv6	CONP/CMNS CLNP/CLNS	AARP	IPX
Acceso a la red	Ethernet PPP Retransmisión de tramas		ATM WLAN	



Puerto	Desc.	Estado	Observaciones
20	FTP	cerrado	Utilizado por FTP
21	FTP	cerrado	Utilizado por FTP
22	SSH	cerrado	Secure Shell.
23	TELNET	cerrado	Acceso remoto
25	SMTP	cerrado	Servidor de correo SMTP
53	DNS	cerrado	Servidor DNS
79	FINGER	cerrado	Servidor de información de usuarios de un PC
80	HTTP	cerrado	Servidor web
110	POP3	cerrado	Servidor de correo POP3
119	NNTP	cerrado	Servidor de noticias
135	DCOM-scm	cerrado	Solo se puede cerrar a través de un cortafuegos
139	NETBIOS	cerrado	Compartición de Ficheros a través de una red
143	IMAP	cerrado	Servidor de correo IMAP
389	LDAP	cerrado	LDAP. Tambien Puede ser utilizado por Neetmeting
443	HTTPS	cerrado	Servidor web seguro
445	MSFT DS	cerrado	Server Message Block.
631	IPP	cerrado	Servidor de Impresion
1433	MS SQL	cerrado	Base de Datos de Microsoft
3306	MYSQL	cerrado	Base de Datos. MYSQL
5000	UPnP	cerrado	En windows está activado este puerto por defecto.

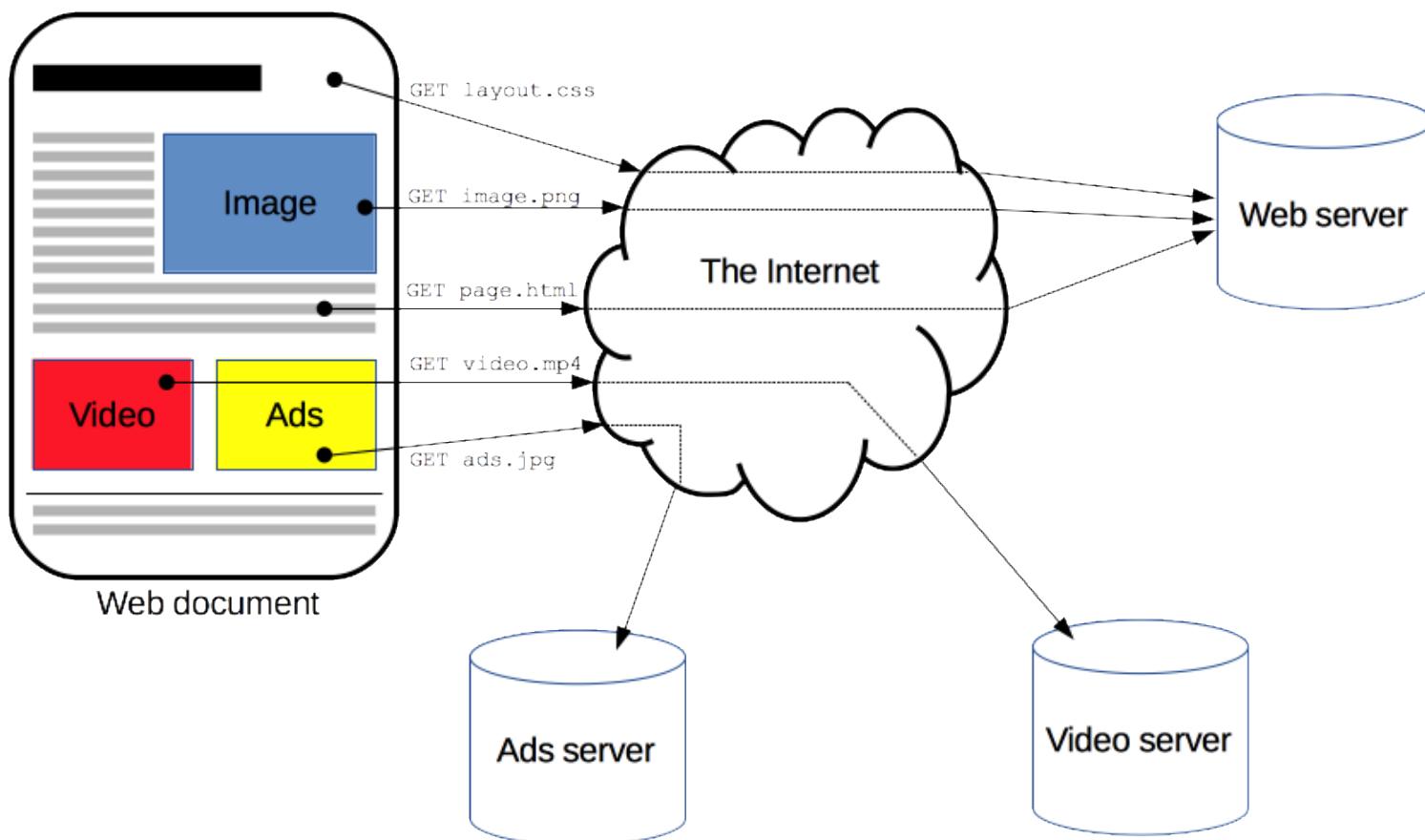
# PROTOCOLO HTTP

- HTTP, de sus siglas en inglés: "Hypertext Transfer Protocol", es el nombre de un protocolo el cual nos permite realizar una petición de datos y recursos, como pueden ser documentos [HTML](#).
- Es la base de cualquier intercambio de datos en la Web, y un protocolo de estructura cliente-servidor, esto quiere decir que una petición de datos es iniciada por el elemento que recibirá los datos (el cliente), normalmente un navegador Web. Así, una página web completa resulta de la unión de distintos sub-documentos recibidos, como, por ejemplo: un documento que especifique el estilo de maquetación de la página web ([CSS](#)), el texto, las imágenes, vídeos, scripts, etc...

# ARQUITECTURA

- Cliente: el agente del usuario
  - El navegador es **siempre** el que inicia una comunicación (petición), y el servidor nunca la comienza
- El servidor Web
  - el cual "*sirve*" los datos que ha pedido el cliente
- Proxies
  - Entre el cliente y el servidor, además existen distintos dispositivos que gestionan los mensajes HTTP.

# CÓMO FUNCIONA ...



- <https://developer.mozilla.org/es/docs/Web/HTTP/Overview>

# FLUJO (I)

- Abre una conexión TCP: la conexión TCP se usará para hacer una petición, o varias, y recibir la respuesta. El cliente puede abrir una conexión nueva, reusar una existente, o abrir varias a la vez hacia el servidor.
- Hacer una petición HTTP: Los mensajes HTTP (previos a HTTP/2) son legibles en texto plano. A partir de la versión del protocolo HTTP/2, los mensajes se encapsulan en franjas, haciendo que no sean directamente interpretables, aunque el principio de operación es el mismo.

```
1 | GET / HTTP/1.1
2 | Host: developer.mozilla.org
3 | Accept-Language: fr
```

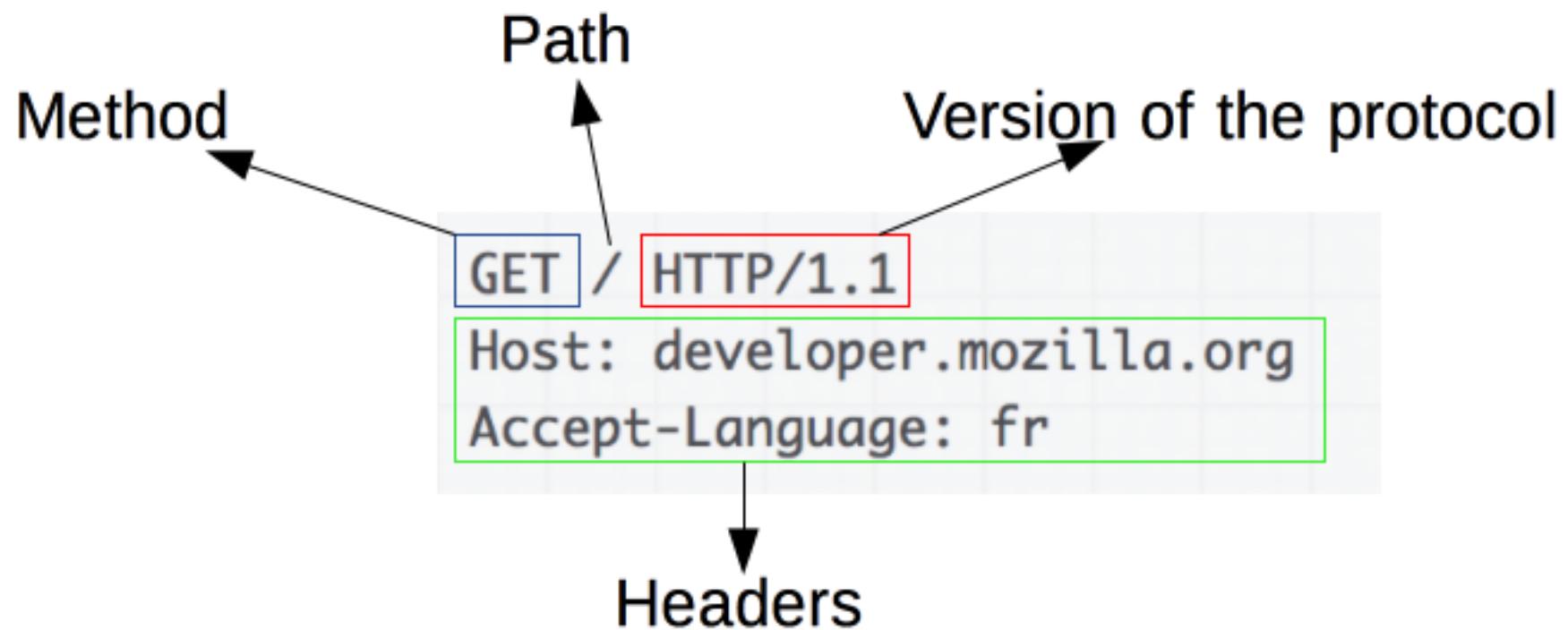
# FLUJO (II)

- Leer la respuesta enviada por el servidor:

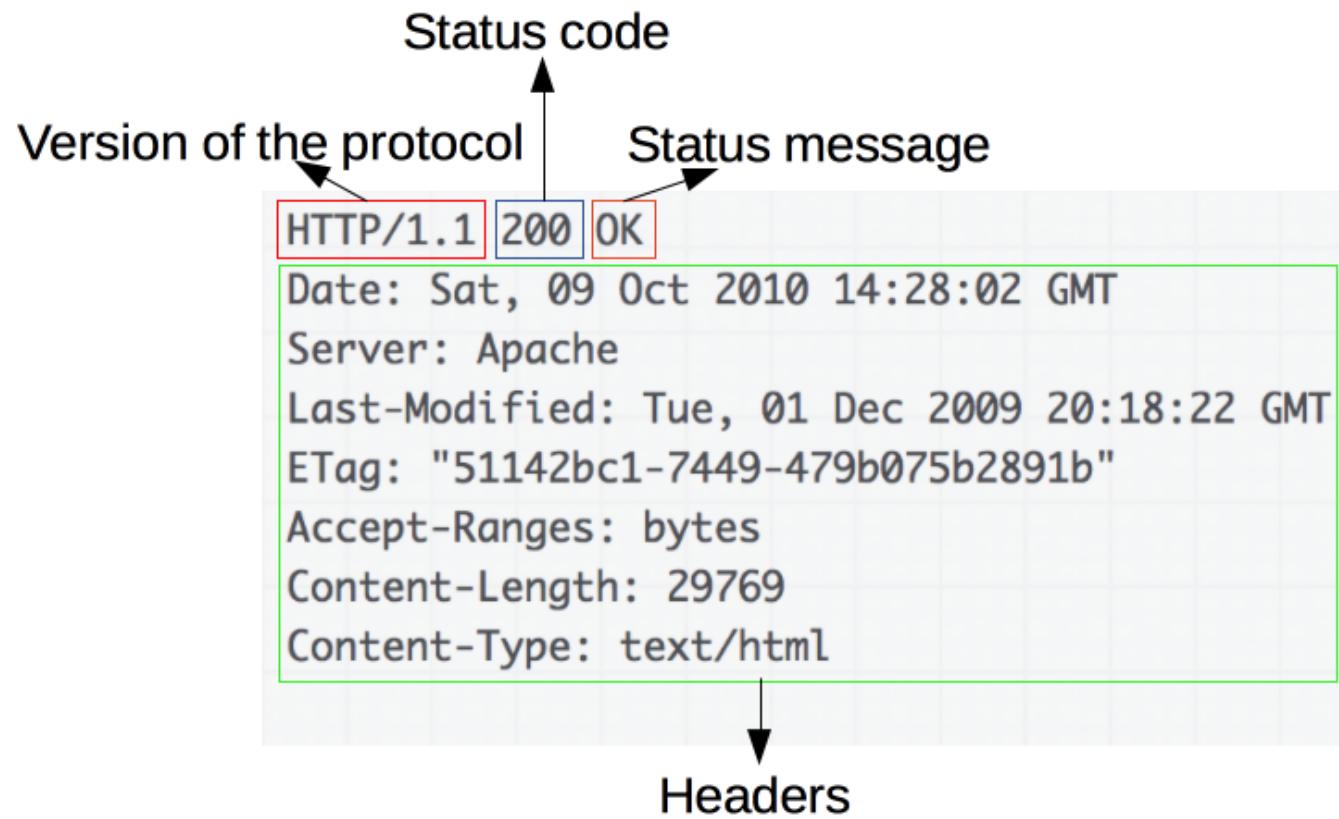
```
1 HTTP/1.1 200 OK
2 Date: Sat, 09 Oct 2010 14:28:02 GMT
3 Server: Apache
4 Last-Modified: Tue, 01 Dec 2009 20:18:22 GMT
5 ETag: "51142bc1-7449-479b075b2891b"
6 Accept-Ranges: bytes
7 Content-Length: 29769
8 Content-Type: text/html
9
10 <!DOCTYPE html...> Here comes the 29769 bytes of the request
```

- CERRAMOS CONEXIÓN

# DESCRIPCIÓN PETICIONES



# RESPUESTAS



# CODIGOS DE ESTADO

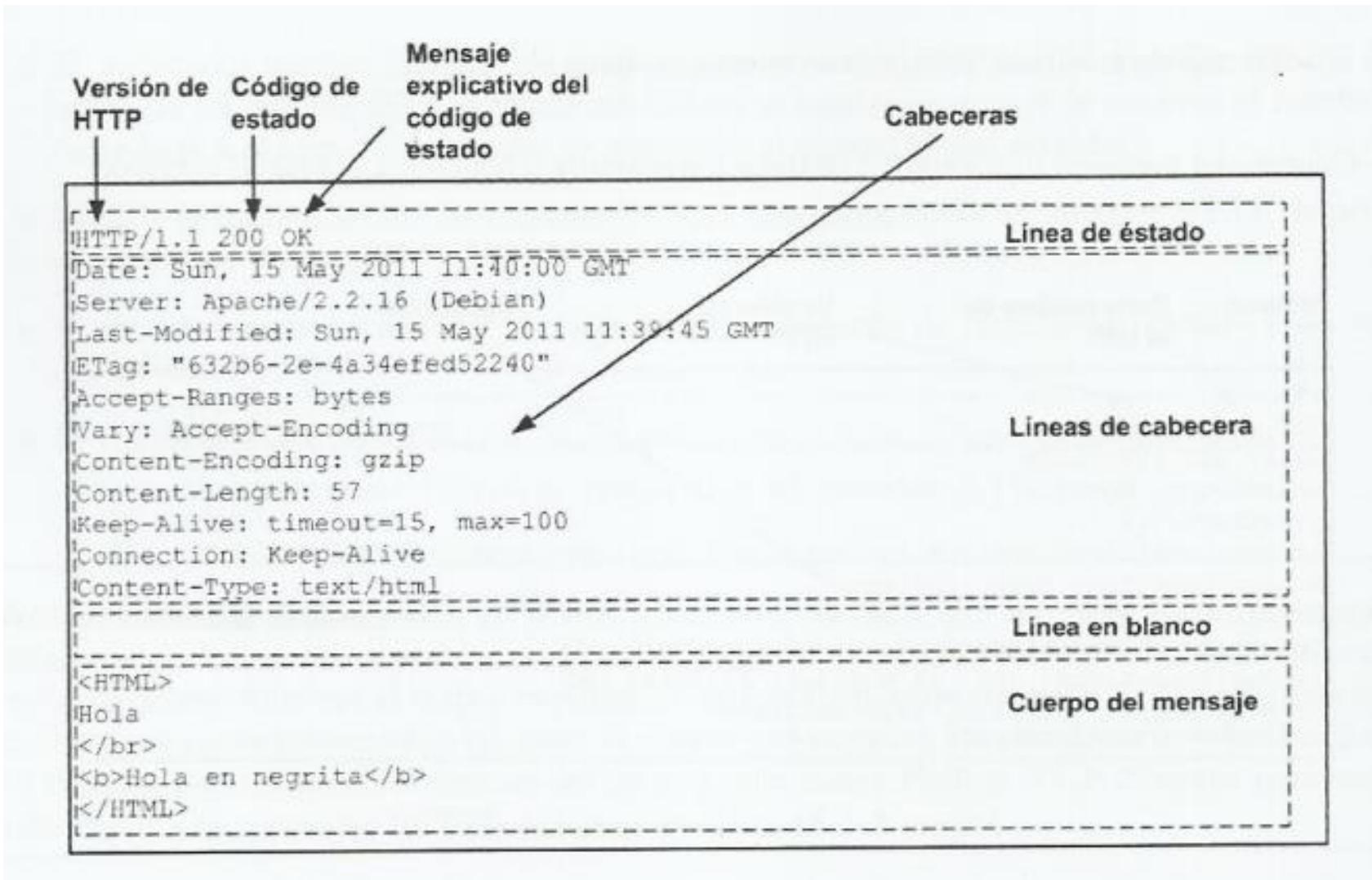
HTTP Status Codes

-  **1xx - Informational** >
-  **2xx - Success** >
-  **3xx - Redirection** >
-  **4xx - Client Error** >
-  **5xx - Server Error** >

# CODIGOS MAS USUALES

- 1xx – Información
  - 100 – Continuar
- 2xx – Éxito
  - 200 – OK
  - 202 – Aceptado
- 3xx – Redirección
  - 301 – Movido permanentemente
  - 302 – Encontrado (redirigir)
  - 307 – Redirección temporal
- 4xx – Error de cliente
  - 400 – Petición errónea
  - 401 – No autorizado
  - 403 – Prohibido
  - 404 – No encontrado
  - 407 – Proxy requiere autentificación
- 5xx – Error de servidor
  - 500 – Error interno
  - 501 – No implementado

# ¿DÓNDE LOS VEMOS?



# CABECERAS

# MÉTODOS

## Tipos de métodos

### HTTP/1.0 (RFC-1945)

- ❖ GET
- ❖ POST
- ❖ HEAD
  - Idéntico al GET, salvo que no se incluye el objeto en el cuerpo de la respuesta (sólo las cabeceras correspondientes)

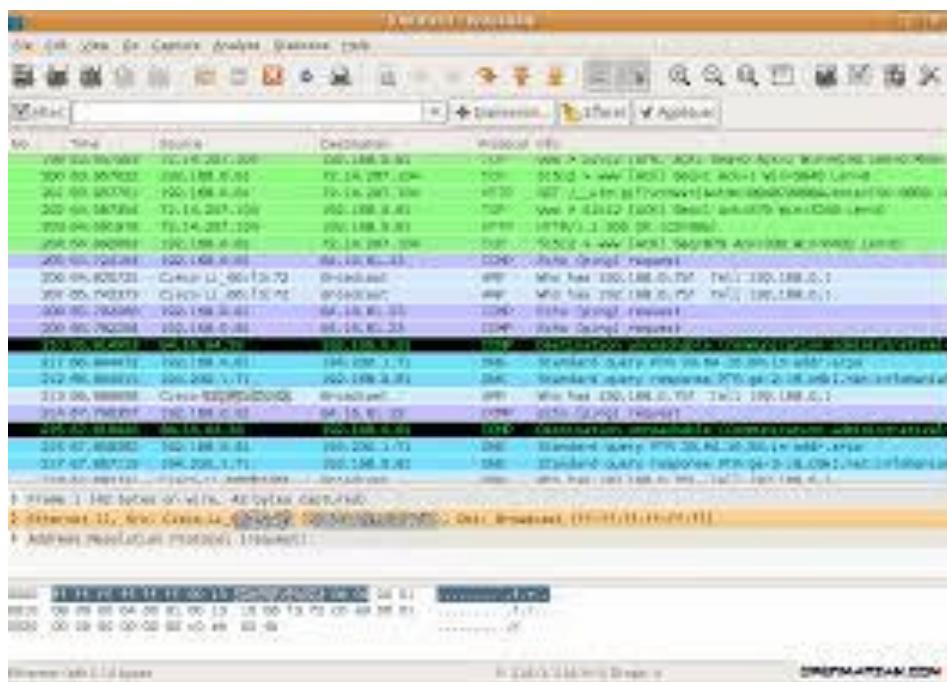
### HTTP/1.1 (RFC-2616)

- ❖ GET, POST, HEAD
- ❖ PUT
  - Sube el fichero en el CUERPO de la petición al path especificado en la URL
- ❖ DELETE
  - Borra del servidor el fichero especificado en la URL

# PÁGINA DE CÓDIGOS

# MONITORIZACIÓN DE MENSAJES HTTP

- [https://developer.mozilla.org/en-US/docs/Tools/Network\\_Monitor](https://developer.mozilla.org/en-US/docs/Tools/Network_Monitor)
- WIRESHARK



## Prueba el HTTP tú mismo

1. Telnet a tu servidor Web favorito:

```
telnet www.dte.us.es 80
```

Abre conexión TCP al puerto 80  
(puerto HTTP por defecto) de www.dte.us.es

Todo lo que escribas se envía allí

2. Escribe una petición GET:

```
GET /docencia/ HTTP/1.1  
Host: www.dte.us.es
```

Escribe esto (con doble-enter al final) para enviar un GET request reducido a un servidor HTTP

3. Mira el mensaje de respuesta del servidor!  
(o puedes usar Wireshark!)

P. ¿Qué ocurre si envío "hola"?