UF5 - Sistemas informáticos en red. Configuración y explotación

SISTEMAS INFORMÁTICOS

Índice

Introducción

Los SSII (*Sistemas Informáticos*) se comunican y comparten información gracias a los sistemas en red. Hoy en día, cualquier SO es capaz de gestionar una red a la que está conectado mediante *hardware* de red.

Para que dos equipos en red puedan comunicarse, es necesario que ambos conozcan los **protocolos de red** necesarios para su comunicación.

Los SSII en red se basan en modelos de referencia que establecen las especificaciones necesarias para que dos equipos intercambien información. Los más utilizados son OSI y TCP/IP, que establecen diferentes capas de comunicación.

- En cada comunicación intervienen múltiples protocolos de red.
- Cada protocolo de red utilizado se ocupa de una parte (capa) de la comunicación.
- Un protocolo de una capa necesita usar protocolos de capas inferiores.

Modelo TCP/IP

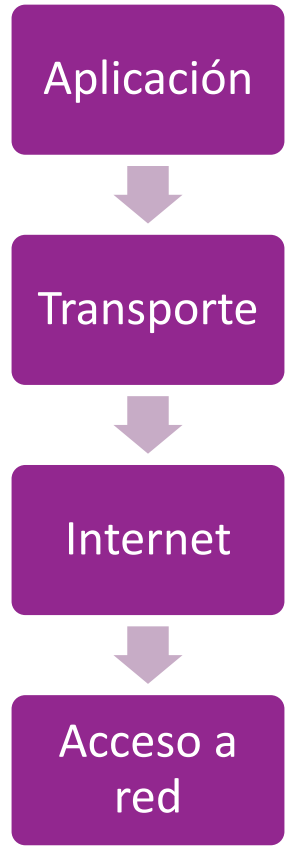
El modelo o arquitectura **TCP/IP** es un conjunto de protocolos creado en los años 70 que define cómo se transmite y encaminan los datos por internet.

Su nombre viene de dos de los protocolos más importantes de internet: TCP e IP, dos de los primeros protocolos definidos en el estándar.

Los protocolos se reparten en 4 capas de la arquitectura, donde las capas más altas acuden a las que tienen debajo para llevar a cabo aspectos específicos de la comunicación.

Por ejemplo:

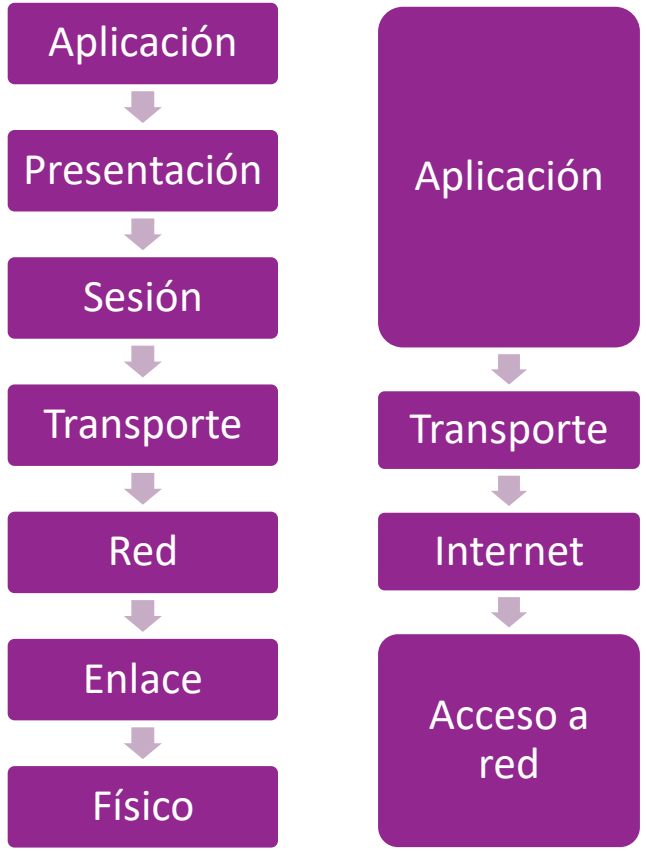
- HTTP usa TCP para transportar los mensajes
- TCP usa IP para encaminar cada paquete
- IP usa el protocolo del medio que esté usando (Ethernet, WiFi, etc.) para comunicar el paquete por dicho medio.



Modelo OSI

El modelo **OSI** se creó como alternativa más estructurada a TCP/IP, aunque no llegó a imponerse.

OSI (*Open System Interconnections*) desgrana la capa de Aplicación en 3 capas y Acceso a red en 2.

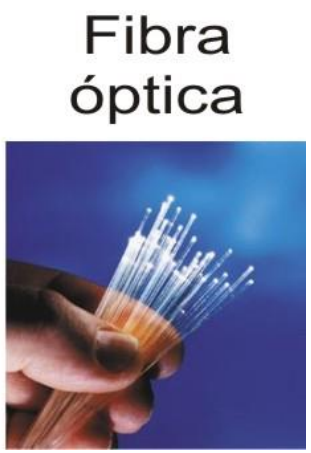


Capa física

En el modelo OSI, la capa física determina las especificaciones mecánicas, eléctricas y funcionales que establece el medio físico de transmisión.

Los principales medios físicos de transmisión son:

- Por cable
  - Cable coaxial
  - Cable de par trenzado (con/sin apantallar)
  - Cable de fibra óptica
- Inalámbrico
  - Wi-Fi
  - 3G/4G/5G
  - Bluetooth
  - NFC

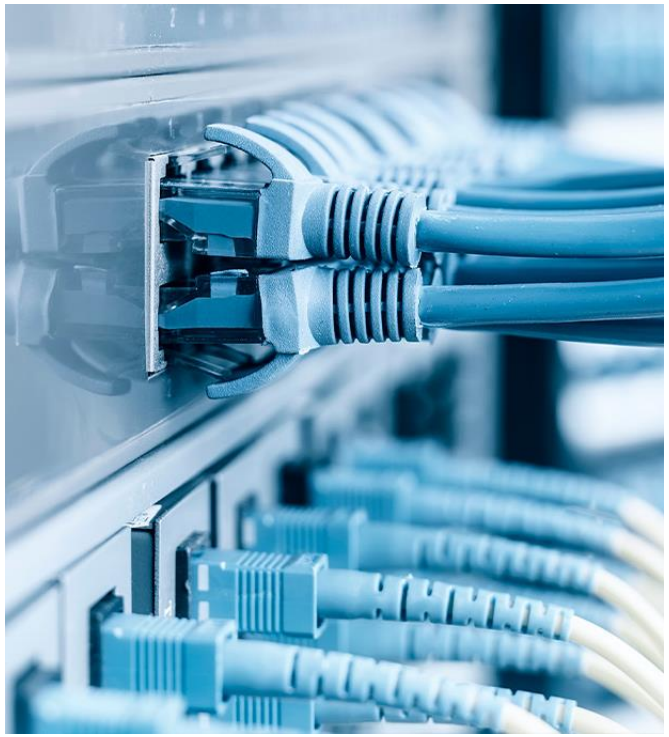


Nivel de acceso a red

La **capa de enlace o acceso a red** es la primera capa de protocolos de la red, la más próxima al **medio físico**.

Especifica el modo en que los datos se van a transmitir por el medio que se va a usar.

Los principales protocolos de esta capa son Ethernet para redes cableadas y Wi-Fi para redes inalámbricas. Otros protocolos son Token Ring, PPP, ARP, etc.

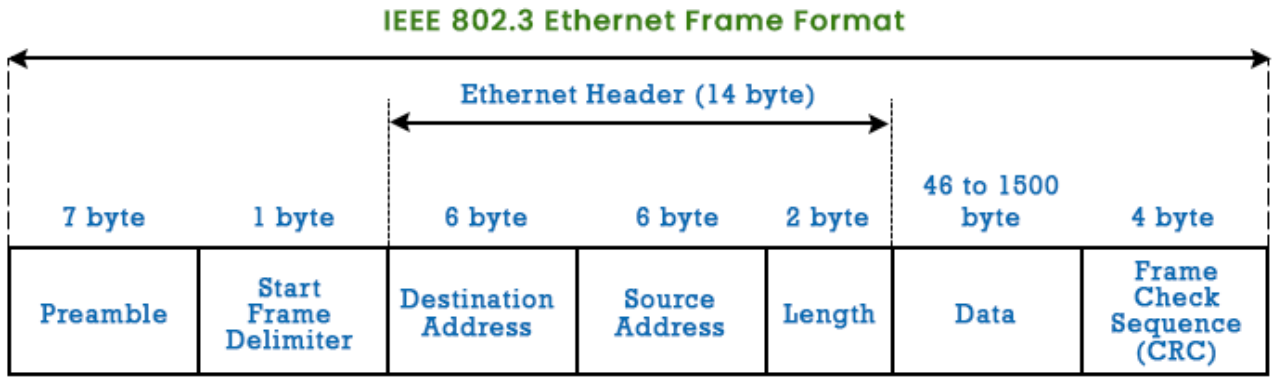


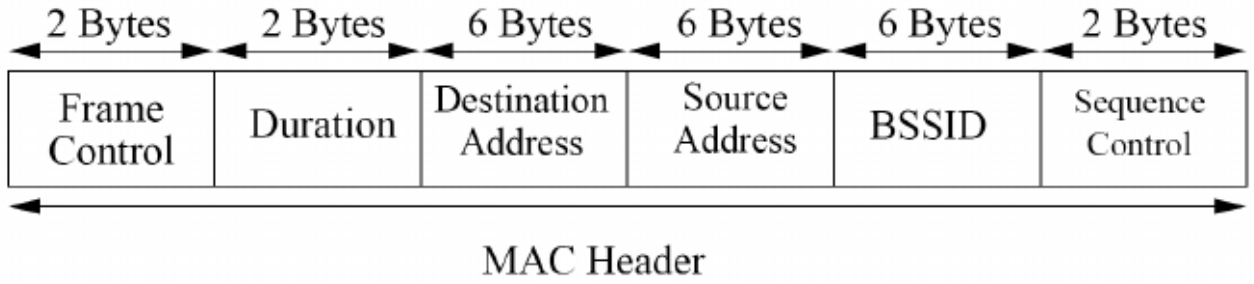
Tramas de acceso a red

La comunicación por cable de red Ethernet se hace mediante **tramas Ethernet**, que tienen la estructura de la primera imagen.

Un ejemplo de **trama Wi-Fi** puede verse en la segunda imagen.

En la capa de enlace se especifican **direcciones MAC de origen y de destino** (entre máquinas vecinas)





Direcciones MAC

Una **dirección física** o **MAC** (*Medium Access Control*) es un identificador de 48 bits (6 bytes) que corresponde de forma única a un **dispositivo de red**.

- Si un equipo tiene una tarjeta de red y una tarjeta WiFi, cada uno tendrá su propia MAC única.

A cada dispositivo de red le asigna su fabricante una dirección MAC globalmente única, es decir, no existe ningún otro dispositivo en el mundo al que le hayan asignado la misma MAC.

Una dirección MAC se representa mediante 12 dígitos hexadecimales divididos en 6 grupos de 2 dígitos separados por dos puntos (**:**).

- Por ejemplo: f2:7f:26:5c:01:29.
- Existe una dirección MAC especial de **difusión** o *broadcast* (ff:ff:ff:ff:ff:ff), que sirve para mandar un paquete a todos los vecinos de la red.

Nivel de internet

En la **capa de red o internet** se realiza el **direccionamiento** de equipos y **encaminamiento** (*routing*) de la información a través de la red.

El protocolo **IP** es el principal de este nivel, aunque también existen algunos otros protocolos como ICMP.

Desde la creación de internet se ha estado usando IP versión 4, **IPv4** (1983), que usa direcciones de 32 bits.

- Ejemplo de dirección IPv4: 192.168.1.110

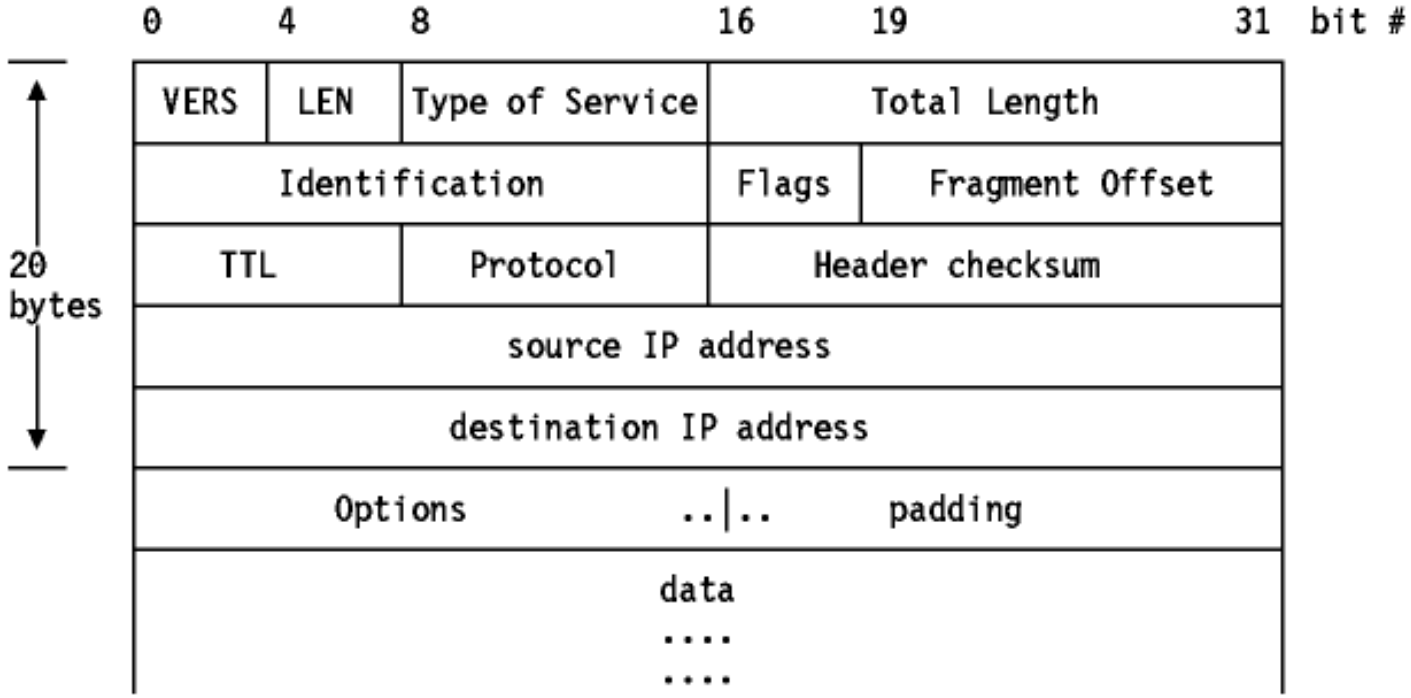
Por falta de direcciones IPv4 (2^{32}, unos 4 mil millones), se publicó **IPv6** (2012), con direcciones de 128 bits, aunque su uso sigue siendo marginal.

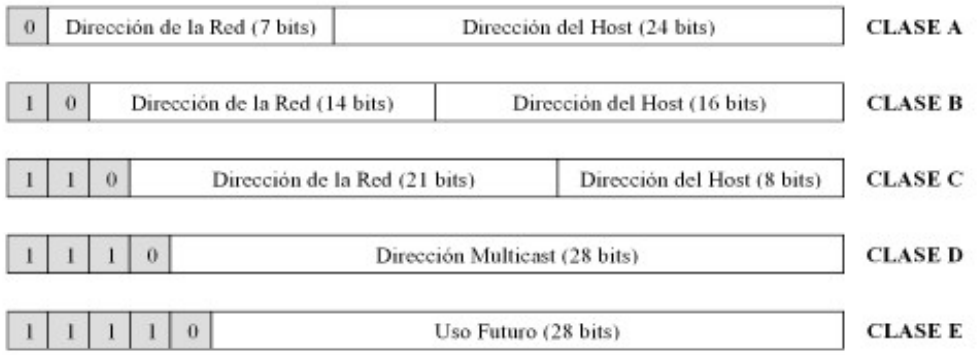
- Ejemplo de dirección IPv6: 2001:0db8:0000:0000:0000:0000:0000:00a3 (o 2001:db8::a3)

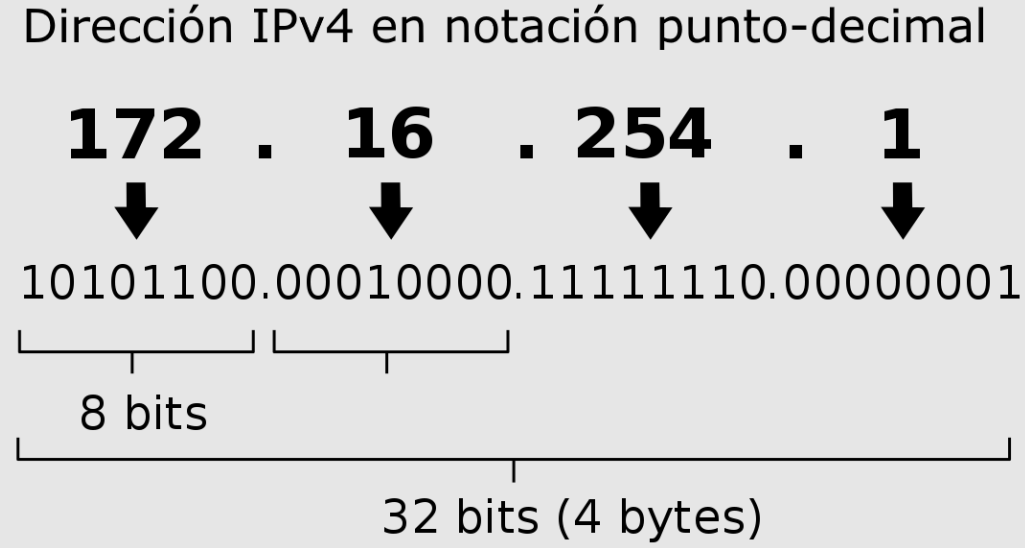
Datagramas IP

La comunicación mediante IP se hace mediante **datagramas IP**, cuya estructura se muestra en la siguiente imagen:

A nosotros nos interesa los campos de **dirección IP de origen y la de destino** (origen del paquete, destino final al que se quiere llevar el paquete).

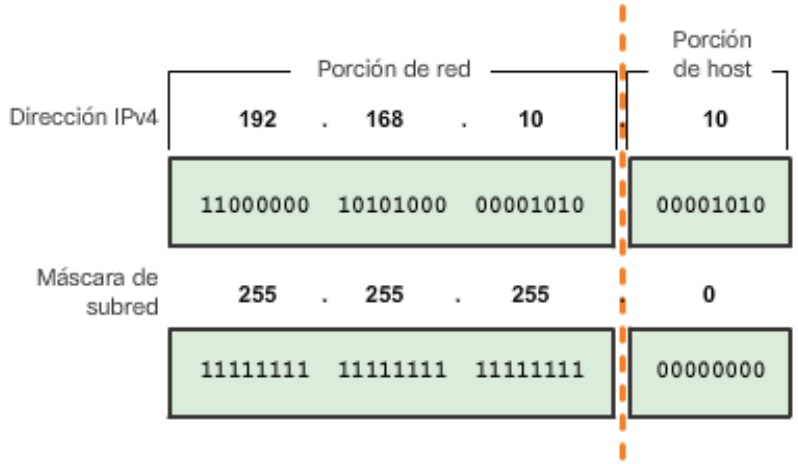






Direccionamiento IPv4

Máscara de subred



La dirección IP tiene dos partes:

- **Identificador de (sub)red** a la que pertenece el equipo.
- **Identificador de equipo o host** dentro de esa red.

Para diferenciarlos, la dirección IP puede venir acompañada de una **máscara de (sub)red**: un número entero de 32 bits con una secuencia de 1's seguida de una secuencia de 0's, donde los 1's marcan los bits de (sub)red y los 0's marcan los bits de host.

- Ejemplo de máscara, con sus distintas representaciones:
  - 11111111 11000000 00000000 00000000 (en bits)
  - 255.192.0.0 (notación punto-decimal)
  - /10 (por la cantidad de bits que tiene a 1)
  - 150.87.0.30/10 (dirección IP + máscara, notación CIDR)
  - Esta máscara nos dice que los 10 primeros bits de la dirección IP identifican la subred y los otros 22 identifican el host.
  - Para conocer su dirección de red, se hace AND lógico de la dirección IP y su máscara.

Direcciones IP especiales

Dirección de red: identifica al conjunto de la red. Todos sus *bits de host* están a 0.

Dirección de difusión (o broadcast) limitada: se emplea para mandar un mensaje de difusión a todos los dispositivos de la propia red. Es la dirección **255.255.255.255**.

Dirección de difusión (o broadcast) dirigida: se emplea para mandar un mensaje de difusión a todos los equipos de una cierta red. Al contrario que una dirección de red, todos sus *bits de host* están a 1.

Dirección de bucle local: sirve para referenciar procesos internos del propio equipo. Es cualquier dirección de la red especial **127.0.0.0/8**. Se suele utilizar la dirección 127.0.0.1 (*localhost*).

Dirección de enlace local: empleada por el protocolo APIPA para establecer una configuración automática de red a equipos a los que no se les ha asignado una. El rango es **169.254.0.0/16**.

Direcciones IP públicas y privadas

Las direcciones IP pueden ser:

- **Públicas**: accesibles desde **internet**.
- **Privadas**: existen rangos de direcciones reservados para redes privadas o **intranets** y no pueden emplearse en internet. Estos rangos son: **10.0.0.0/8**, **172.16.0.0/12** y **192.168.0.0/16**.

Encaminamiento IP

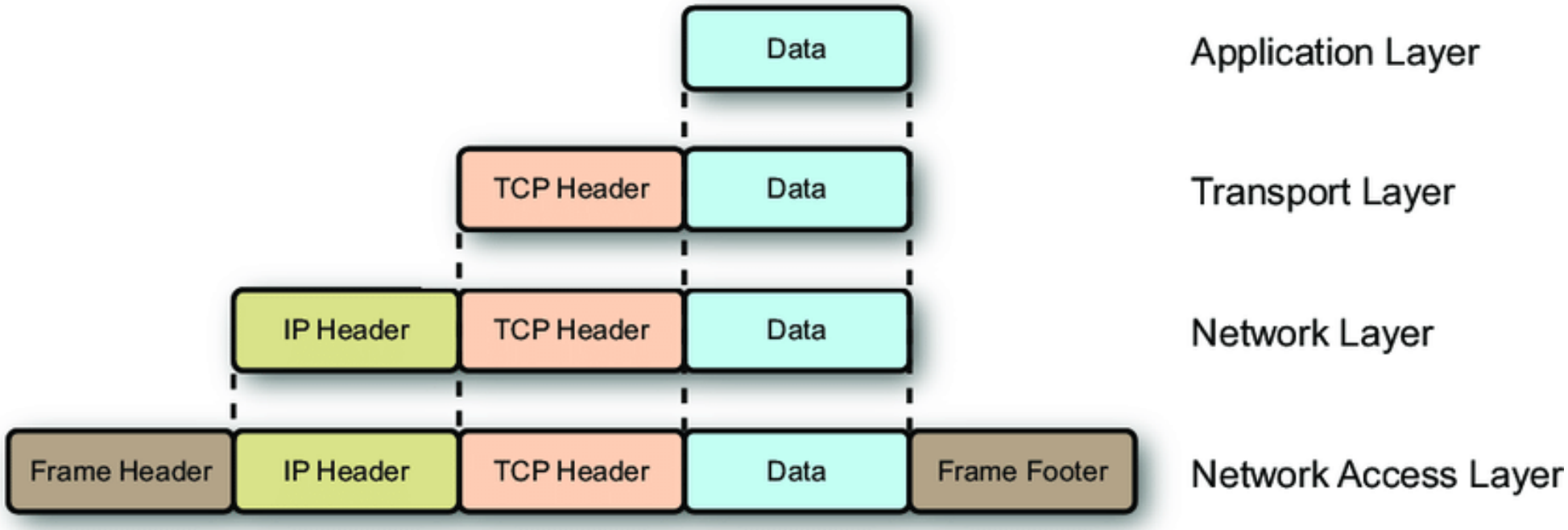
El **encaminamiento** o **enrutamiento** (*routing*) a nivel IP consiste en el proceso de llevar un datagrama IP desde una máquina origen a una máquina destino, aunque ambas se encuentren en diferentes redes. El protocolo IP es el responsable del encaminamiento.

Los **encaminadores** o **routers** son dispositivos de nivel 3 (red) que enlazan las redes de las que forman parte, y encaminan los paquetes entre una y otra mediante **tablas de encaminamiento**.

Los propios equipos también participan en el encaminamiento (del tráfico saliente), ya que si el destino de un paquete pertenece a la misma red, se lo envía directamente, y si no, lo envía a su encaminador (puerta de enlace), que se encargará de llevarlo a su destino.

Cuando el router recibe un datagrama:

- Si va dirigido a una dirección de una red conectada al router, lo entrega al destino directamente.
- Si no, lo reenviará a otro router según su tabla de encaminamiento



Encapsulación

Cada protocolo aporta una cabecera (y, a veces, un pie) al paquete que transporta.

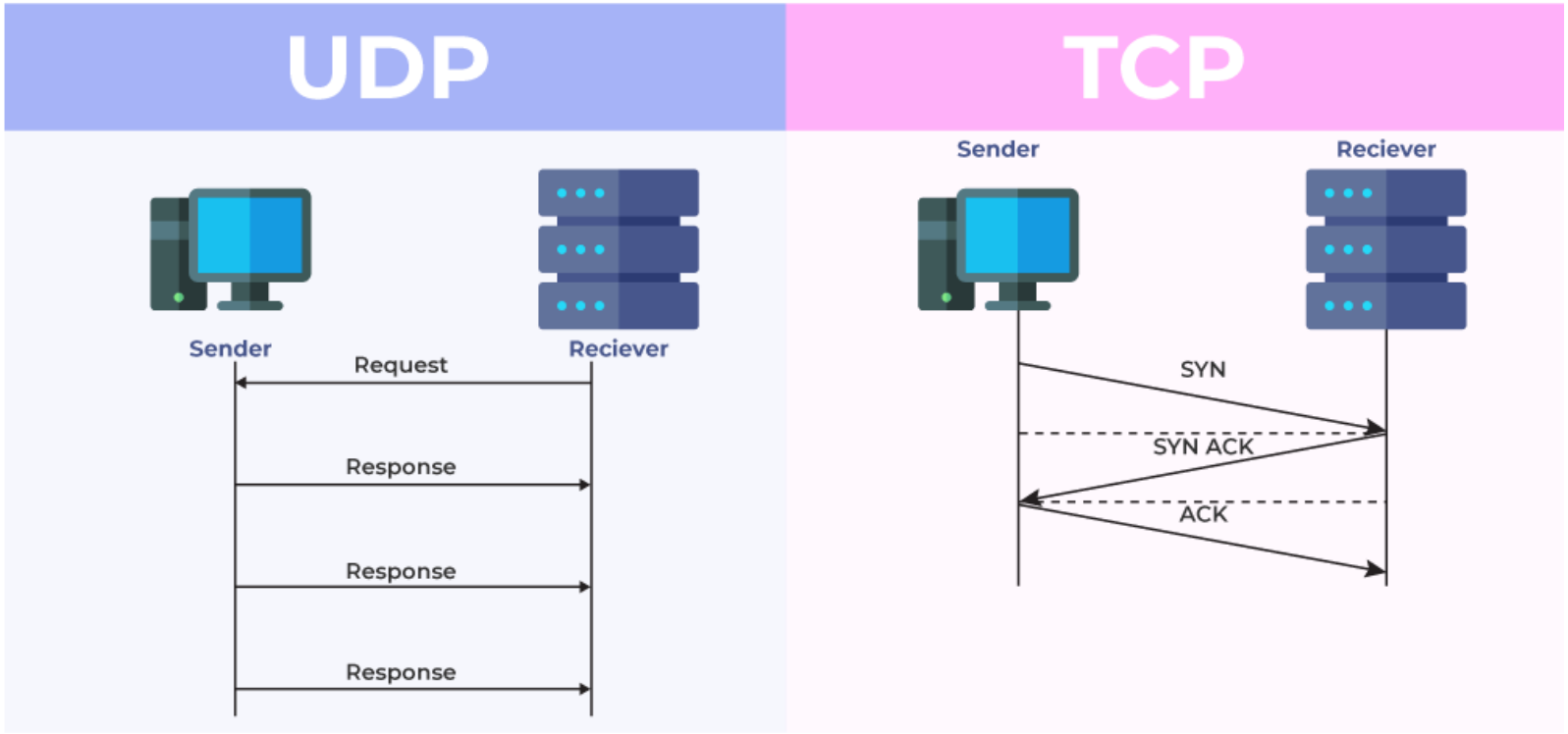
El diagrama de arriba muestra la forma de encapsular un paquete de aplicación al salir de una tarjeta de red.

Nivel de transporte

El protocolo IP no nos permite mantener múltiples procesos de comunicación simultáneos dentro de la misma máquina.

La **capa de transporte** permite diferenciar y gestionar múltiples orígenes y destinos en una comunicación mediante la asignación de **puertos**, identificar extremos finales mediante *sockets* (IP + puerto) y trocear mensajes grandes en múltiples paquetes. Otras posibles prestaciones propias de esta capa son, además, mantener una conexión, asegurar el orden de llegada de los paquetes e incluso proporcionar autenticación y cifrado.

Los dos protocolos básicos de transporte son **TCP y UDP**.



TCP y UDP

UDP (*User Datagram Protocol*):

Es el más básico, **solo envía el paquete**. No es fiable, pero es rápido. Se usa para DHCP, DNS, *streaming*, etc.

TCP (*Transmission Control Protocol*):

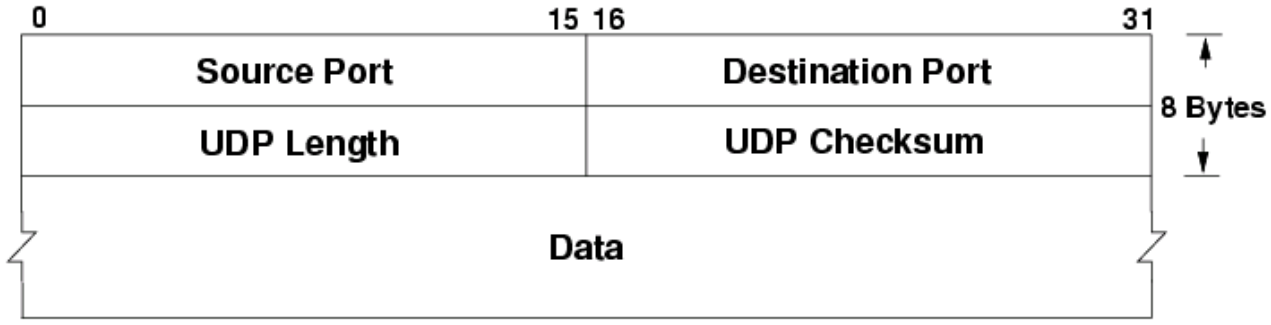
Proporciona un servicio **orientado a conexión**, con control de flujo y de errores, por lo que es **fiable** y **lento**. Establece conexión (*handshake*), envía confirmaciones de recepción y reenvía los paquetes perdidos. Se usa para HTTP, FTP, SMTP, SSH, etc.

Datagramas de transporte

El diagrama de arriba muestra la cabecera de un paquete TCP, y la de abajo, la de UDP:

A nosotros nos interesa los campos de **dirección de puerto de origen y de destino**.

TCP Header				
Bits	0-15			16-31
0	Source port			Destination port
32	Sequence number			
64	Acknowledgment number			
96	Offset	Reserved	Flags	Window size
128	Checksum			Urgent pointer
160	Options			



Nivel de aplicación

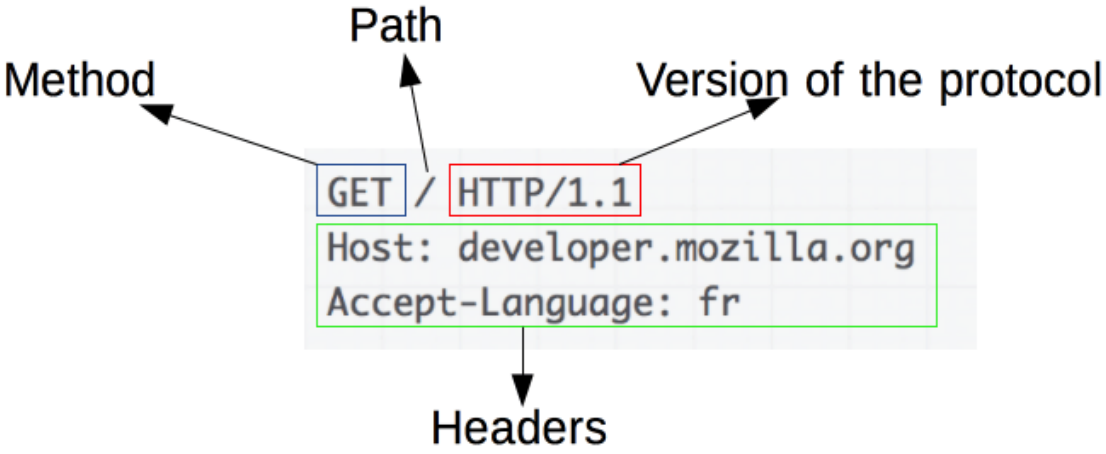
La **capa de aplicación** es la capa superior de la arquitectura TCP/IP, ya que representa a las aplicaciones que usarán TCP o UDP por debajo.

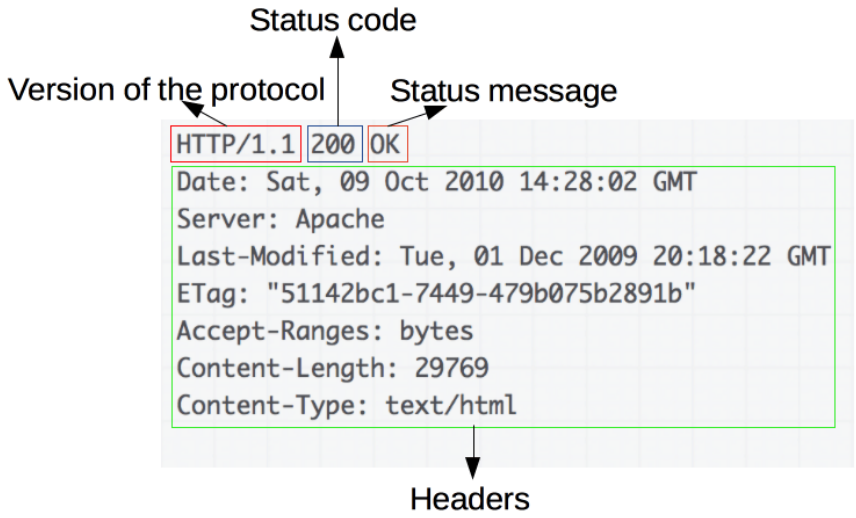
Ejemplos: HTTP, Telnet, FTP, SMTP, DNS, SMTP, IMAP, etc.

Cada protocolo de este nivel se configura utilizando algún puerto TCP o UDP.

Paquetes HTTP

Los siguientes son ejemplos de paquetes de petición/respuesta HTTP con cabeceras:





Paquetes SMTP

El siguiente es un ejemplo de paquete SMTP con un mensaje y cabeceras: