

Despliegue de aplicaciones WEB

TEMA 1

Arquitectura de red por niveles

Juan Antonio López Mera
IES VELÁZQUEZ

0. Índice

- 1. La necesidad de la arquitectura de red por niveles*
- 2. Modelo OSI*
- 3. Protocolo TCP/IP*
- 4. Bibliografía*

1. La necesidad de la arquitectura de red por niveles

- La utilización de distintas implementaciones tanto a nivel de hardware como de software hacían difícil la compatibilidad a la hora de comunicarse entre distintos dispositivos.
- Se hizo necesario el uso de unos estándares para posibilitar la información entre distintos dispositivos de distintos fabricantes.
- Los estándares se aplicaron de manera separada para los distintos niveles que forman parte de un proceso de comunicación: cada nivel se denomina capa.
- De manera teórica, en el año 1984, se propuso el modelo OSI. Y en este modelo se basa la arquitectura usada mundialmente: arquitectura TCP/IP.

2. Modelo OSI

¿Qué es?

- Significa Modelo de Interconexión de Sistemas Abiertos
- Es el resultado de un estudio teórico en el que se define una estructura de una arquitectura de red con 7 capas o niveles.
- Define las capas, pero nunca ha sido implementado, aunque ha servido de modelo para otras arquitecturas por capas que sí han sido implementadas (TCP/IP, AppleTalk, NetBEUI).

- Las capas son:



2. Modelo OSI

Capa 7: Aplicación

- Es la capa más cercana al usuario.
- Proporciona la interfaz desde donde el usuario se comunica en la red.
- Forman parte de esta capa:
 - Aplicaciones como **navegadores** o **clientes de correo**
 - Servicios de **transferencia de archivos**, **prioridad en la red**.
 - Protocolos como **DNS, HTTP, SMTP, Telnet, FTP**.



2. Modelo OSI

Capa 6: Presentación

- Se encarga de que el el formato de los datos sea el adecuado
- También es la encargada de que la información que se envía pueda ser leída por la capa de aplicación de destino (algo así como una traductora de formatos para que capas de aplicación y destino se entiendan).
- Realiza tareas de cifrado y compresión de datos.



2. Modelo OSI

Capa 5: Sesión

- Como su propio nombre indica, coordina el diálogo por medio de aperturas de sesión durante la comunicación (establece, usa y finaliza la conexión).
- También sincroniza la comunicación y la transferencia de datos.
- Administra el testigo durante el proceso de comunicación.



2. Modelo OSI

Capa 4: Transporte

- Controla el flujo de datos durante la comunicación, controlando que lleguen sin errores, en orden y descartando duplicados.
- En el envío, recibe los datos de la capa de sesión, los fragmenta y los pasa a la capa de red (paquetes).
- En la recepción, recibe los paquetes, los ensambla y los pasa a la capa de sesión.



2. Modelo OSI

Capa 3: Red

- La estructura de datos que utiliza se denomina PAQUETE.
- Elige la mejor ruta a seguir entre origen y destino de los paquetes (enrutadores y nodos intermedios).



2. Modelo OSI

Capa 2: Enlace de datos

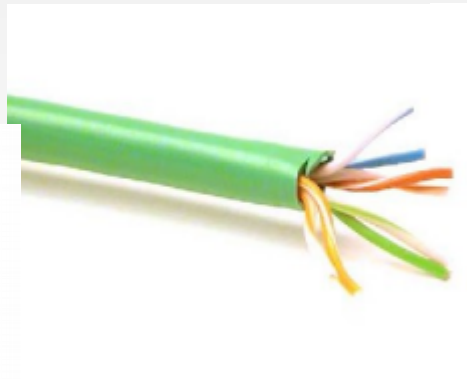
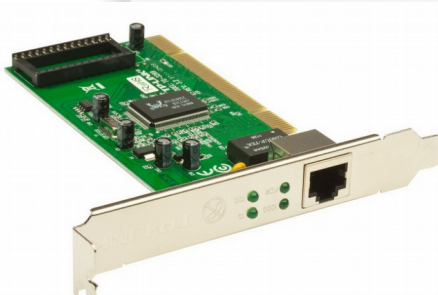
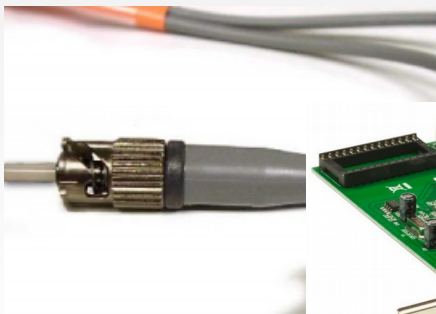
- La estructura de datos que utiliza se denomina TRAMA
- Proporciona un tránsito de datos confiable a través del medio físico (controla errores y verifica la integridad de los datos).
- También se encarga del direccionamiento físico (switch) añadiendo información sobre el origen y el destino de los datos.
- Convierte los bits que vienen de la capa física en tramas y viceversa.



2. Modelo OSI

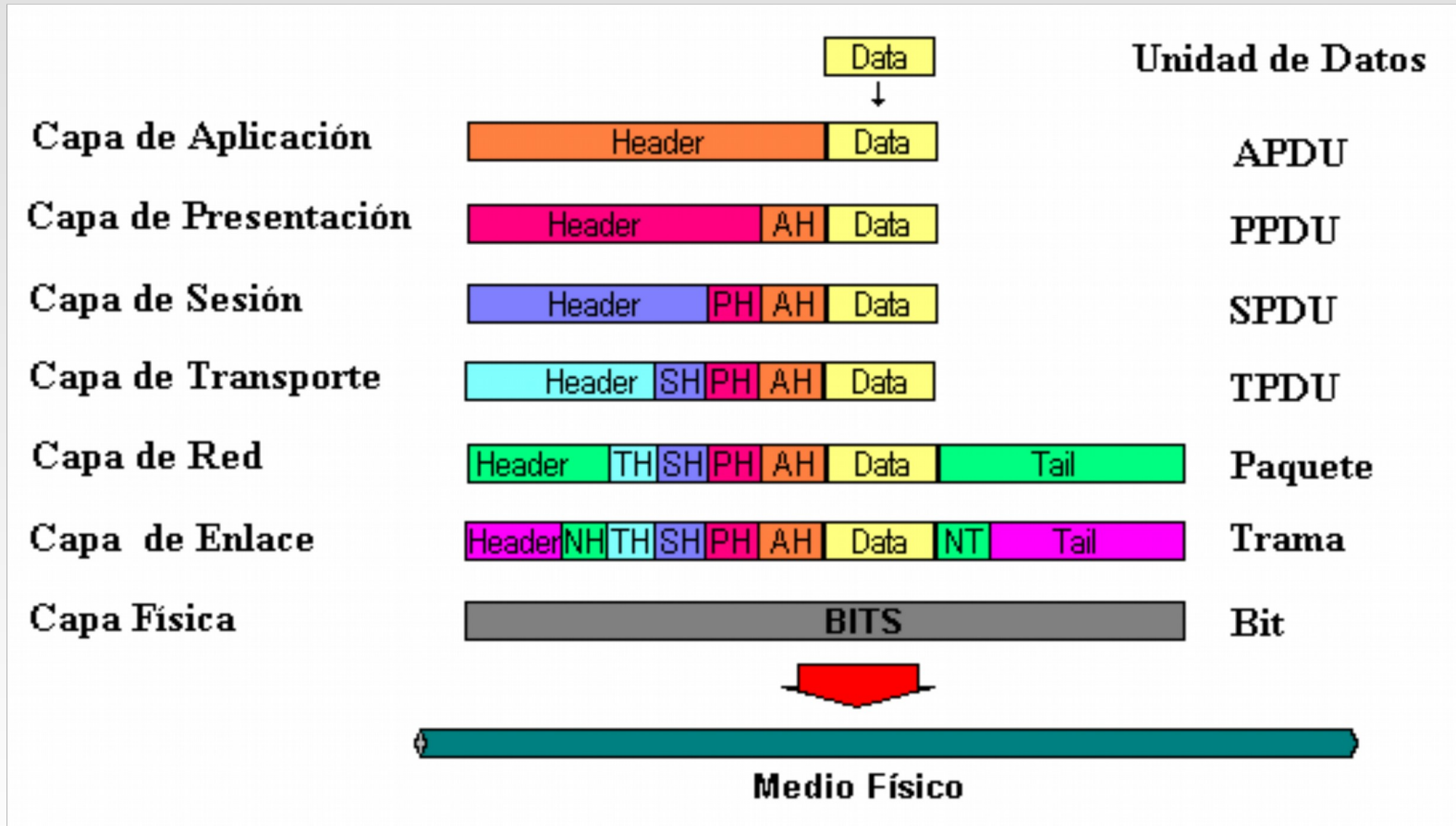
Capa 1: Física

- Usa directamente BITS.
- Define las características físicas y eléctricas de la comunicación (distancia máxima permitida para la comunicación, voltaje del 1 y voltaje del 0...).
- Se encarga de la transmisión física de datos a través de la red.



2. Modelo OSI

Encapsulación



3. Protocolo TCP/IP

¿Qué es?

- Protocolo de comunicación entre dispositivos en Internet.
- Significa: Transmission Control Protocol / Internet Protocol
- Permite la comunicación entre dispositivos de forma que:
 - No tienen por qué tener compatibilidad de hardware/software
 - Es tolerante a fallos
 - Es fiable

3. Protocolo TCP/IP

Capas OSI vs Capas TCP/IP

Modelo TCP/IP	Modelo OSI
Aplicación	Aplicación
	Presentación
	Sesión
Transporte	Transporte
Internet	Red
Acceso a red	Enlace de datos
	Física

3. Protocolo TCP/IP

Capas OSI vs Capas TCP/IP

- **Capa aplicación:** Los protocolos de nivel superior deberían incluir los detalles de las capas de aplicación, presentación y sesión del modelo OSI (protocolos alto nivel, representación, codificación y control de diálogo).
- **Capa de transporte (TCP):** Se encarga de la confiabilidad, control de flujo y corrección de errores.
- **Capa de internet (IP):** Se encarga del envío de paquetes de origen a destino independientemente de la ruta tomada.
- **Capa de acceso a red:** Se encarga de la tecnología LAN, WAN y de todos los detalles físicos de la comunicación.

3. Protocolo TCP/IP

Protocolos

- Alberga más de 100 protocolos distintos, entre los que destacamos:
 - TCP (Transmission Control Protocol)
 - UDP (User Datagram Protocol)
 - IP (Internet Protocol)
 - ICMP (Internet Control Message Protocol)
 - DHCP (Dinamic Host Configuration Protocol)

3. Protocolo TCP/IP

TCP

- Permite la comunicación entre dos dispositivos a partir de una conexión previa.
- Se realiza a partir de una petición de comunicación de la aplicación que la requiere (handshake).
- Cuando la aplicación receptora la acepta se establece una conexión “full-duplex” (en el momento que una de las dos partes cierra la conexión se pierde la comunicación).
- Cada lado de la conexión tiene diversos puertos abiertos o “a la escucha”. Algunos son FTP(21), SSH(22), Telnet (23), SMTP(25) y HTTP(80).
- Fiable, aunque lenta.

3. Protocolo TCP/IP

UDP

- Permite la comunicación entre dos dispositivos sin necesidad de una comunicación previa
- La información se envía a través de DATAGRAMAS, donde aparecen los datos necesarios como para que no sea necesaria una conexión previa.
- Usado para el envío masivo de datos, como por ejemplo, audio y vídeo.
- Es más importante la velocidad de envío de datos que la seguridad.
- En las máquinas también existen puertos UDP “a la escucha”.

3. Protocolo TCP/IP

Rango de puertos TCP

- Tiene una longitud de 16 bits, por lo que existen 65535 puertos.
 - Del 0 al 1023 se llaman puertos bien conocidos (se usan para protocolos bien conocidos, como el 80 para HTTP). Para usarlos debemos ser superusuarios o administradores.
 - Del 1024 al 49151 son puertos registrados. Pueden ser usados por cualquier aplicación.
 - Del 49151 son puertos temporales. Se usan en conexiones punto a punto.

3. Protocolo TCP/IP

IP

- Transmisión de datos por PAQUETES conmutados no fiables.
- No hay forma de conocer si un paquete llega a su destino.
- Las cabeceras IP contienen las direcciones de las máquinas origen y destino que serán usadas por los enrutadores para decidir el tramo de red por donde envían los paquetes.
- Los protocolos son IPv4 e IPv6

3. Protocolo TCP/IP

IP

- Los campos que forman la cabecera IP son:

- Versión (v4,v6)
- Longitud de cabecera
- Tipo de servicio(para indicar la prioridad o importancia de los datos)
- Longitud total
- Identificación
- Flags
- Fragmentación
- Límite de existencia (para descartar el paquete si no llega a su destino).
- Protocolo de transmisión (TCP,UDP)
- Comprobación (checksum de las IP's pero no de los datos).
- Dirección origen
- Dirección destino

Formato de la Cabecera IP (Versión 4)				
0-3	4-7	8-15	16-18	19-31
Versión	Tamaño Cabecera	Tipo de Servicio	Longitud Total	
Identificador			Flags	Posición de Fragmento
Time To Live		Protocolo	Suma de Control de Cabecera	
Dirección IP de Origen				
Dirección IP de Destino				
Opciones				Relleno

3. Protocolo TCP/IP

Dirección IP

- Identifica de manera lógica un dispositivo conectado a una red (la identificación física es la dirección MAC de una tarjeta de red).
- Dirección IP dinámica: un dispositivo no siempre tiene por qué usar la misma dirección IP, sino que es asignada por un servidor DHCP.
- Dirección IP estática: un dispositivo tiene asociada, siempre que se conecta a la red, la misma dirección IP.
- Los servidores DNS asocian sinónimos a las direcciones IP para que sean más fácilmente reconocibles por los usuarios a la hora de conectar con éstos.

3. Protocolo TCP/IP

IPv4

- Número de 32 bits (separados en octetos por el carácter “.”) único para cada host dentro de una red.
- **IP privada:** identifica al dispositivo dentro de la red.
- **IP pública:** identifica a la red fuera de la red (Internet). Todos los dispositivos de la red comparten la misma IP pública.



3. Protocolo TCP/IP

IPv4: Clases

[illegible]

3. Protocolo TCP/IP

IPv4: direcciones especiales

- **Broadcasting**: se envía el mensaje a todos los dispositivos de una misma red.
- **Loopback**: 127.x.x.1. Se utiliza para comprobar que los protocolos TCP/IP están funcionando en nuestro dispositivo.
- **0.0.0.0** : el dispositivo no tiene aún asignada ninguna dirección IP por parte de la red.

3. Protocolo TCP/IP

IPv4: subnetting y máscara de red

- Cuando queremos crear redes independientes dentro de una misma red aplicamos la técnica de subnetting, en la cual los bits de host son usados como bits de red..
- La máscara de red es la encargada de identificar los bits utilizados para red y los utilizados para hosts.

Class A	Network	Host	Host	Host
Subnet Mask	255	0	0	0

Class B	Network	Network	Host	Host
Subnet Mask	255	255	0	0

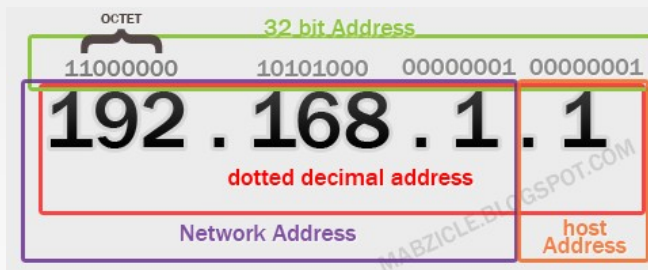
Class C	Network	Network	Network	Host
Subnet Mask	255	255	255	0

www.smartPctricks.com

3. Protocolo TCP/IP

IPv6

- Compuesta por 128 bits (en IPv4 eran 32).
- Se representa en hexadecimal y cada bloque de 16 bits se separa por el símbolo “:”
- Los bloques contiguos de 0's se obvian escribiendo ::



Una dirección IPv6 (en hexadecimal)

2001:0DB8:AC10:FE01:0000:0000:0000:0000

↓ ↓ ↓ ↓

2001:0DB8:AC10:FE01:: Se pueden omitir los ceros

1000000000000001:0000110110111000:1010110000010000:1111110000000001:
0000000000000000:0000000000000000:0000000000000000:000000000000

3. Protocolo TCP/IP

Protocolo de resolución directa: ARP (Address Resolution Protocol)

- Responsable de encontrar la dirección física MAC a partir de la IP.
- Los hosts disponen en caché de una tabla de correspondencia entre las direcciones IP y las MAC.
- Si un host quiere enviar un paquete a otro host y no tiene registrada la dirección MAC de éste, envía un broadcasting para almacenarla y guardarla en su tabla.
- El resto de hosts usan esa señal de broadcasting enviada para actualizar su tabla (si fuera necesario) antes de desechar el paquete.

3. Protocolo TCP/IP

Protocolo de resolución inversa: RARP (Reverse Address Resolution Protocol)

- Responsable de encontrar la dirección IP a partir de la dirección MAC.
- En cada red debe existir al menos un servidor RARP que contenga las tablas de correspondencia IP-MAC de manera permanente.
- La información proporcionada por el servidor RARP se limita a la dirección IP, obviando máscara de subred y puerta de enlace.
- RARP deriva a BOOTP : este protocolo de arranque permite la resolución inversa sin necesidad de tablas de correspondencia, además devuelve también la información de la máscara de red y gateway.

4. Bibliografía

Servicios de Red e Internet. Álvaro García Sánchez, Luis Enamorado Sarmiento, Javier Sanz Rodríguez. Editorial Garceta

www.Wikipedia.org

www.exa.unicen.edu.ar/catedras/comdat1/material/ElmodeloOSI.pdf