

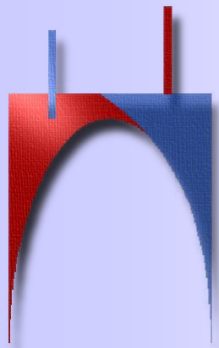
C.F.G.S.

Desarrollo de Aplicaciones Multiplataforma

Desarrollo de Aplicaciones Web

# UD 8

## Fundamentos de Redes



Instituto de Educación Secundaria  
**Santiago Hernández**  
*Informática*

# Introducción:

## ➤ Red de ordenadores

- Conjunto de ordenadores independientes conectados entre sí
- Cada uno puede poner a disposición del resto ciertos recursos de los que dispone:
  - Espacio en disco
  - Impresoras
  - Conexiones
  - ...
- Para acceder a uno de esos recursos se debe conocer, exactamente, la ubicación y el nombre del recurso.
- Esos recursos se denominan **remotos** y el ordenador dispone de un redirector para cuando deba utilizarlos en lugar de los recursos **locales**

## ➤ Formas de organización de las redes

- Grupo de trabajo
  - Todos los equipos son “iguales” y ponen recursos a disposición de los demás
- Cliente-Servidor
  - Existen ordenadores especializados para dar los recursos (**servidores**) que tienen sistemas operativos especiales (de red)
  - En este tipo de arquitectura se pueden establecer sistemas de seguridad basados en usuarios.

## ➤ **Sistemas Distribuidos**

- Por una parte es un sistema similar al de red en la arquitectura cliente-servidor
- Existe más de un ordenador servidor
- El sistema Operativo establecerá en que ordenador deben realizarse las tareas solicitadas por los clientes de forma que se realicen de la forma más eficiente posible
- Los clientes no saben cuantos ordenadores servidores hay ni en cual de ellos se encuentra el recurso al que deben acceder.

# Razones para la utilización de redes

## ➤ Redes para empresas

- Compartir recursos sin que importe su localización
- Alta confiabilidad: pueden existir fuentes alternativas que asumirán el trabajo si fallan otras
- Ahorro: la arquitectura de red es más barata que un mainframe
- Escalabilidad: es sencillo añadir nuevos clientes y servidores.

## ➤ Redes para la gente

- Acceso a información remota: telebanco, telecompra, información, ...
- Comunicación persona a persona: email, videoconferencia, ...
- Entretenimiento interactivo: videos, juegos, ...

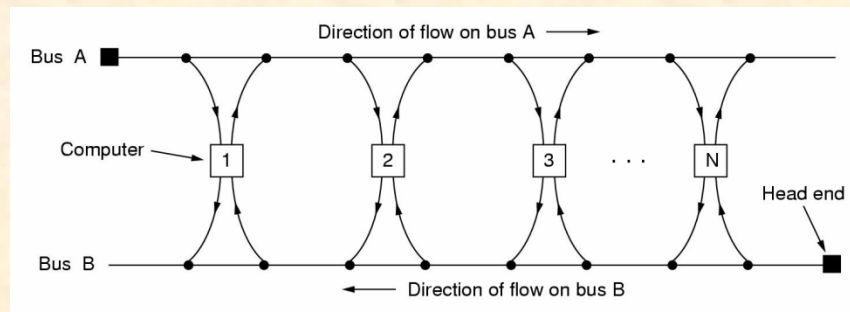
# Clasificación

## ➤ Por tecnología de conexión

- **Redes de Difusión**
  - Un solo canal de comunicación compartido por todos los equipos.
  - La información es recibida por todos los equipos conectados al canal, comprueban si les corresponde y, si no es así, la ignoran.
  - Puede mandarse información a un grupo de equipos (multicast) o a todos (broadcast).
- **Redes Punto a Punto**
  - Las máquinas se conectan de forma directa de una a otra.
  - Si se quiere mandar información desde una máquina a otra y no se tiene conexión directa con ellas se pueden utilizar otras máquinas como pasos intermedios. En estos casos es necesario implementar algoritmos de **encaminamiento**.

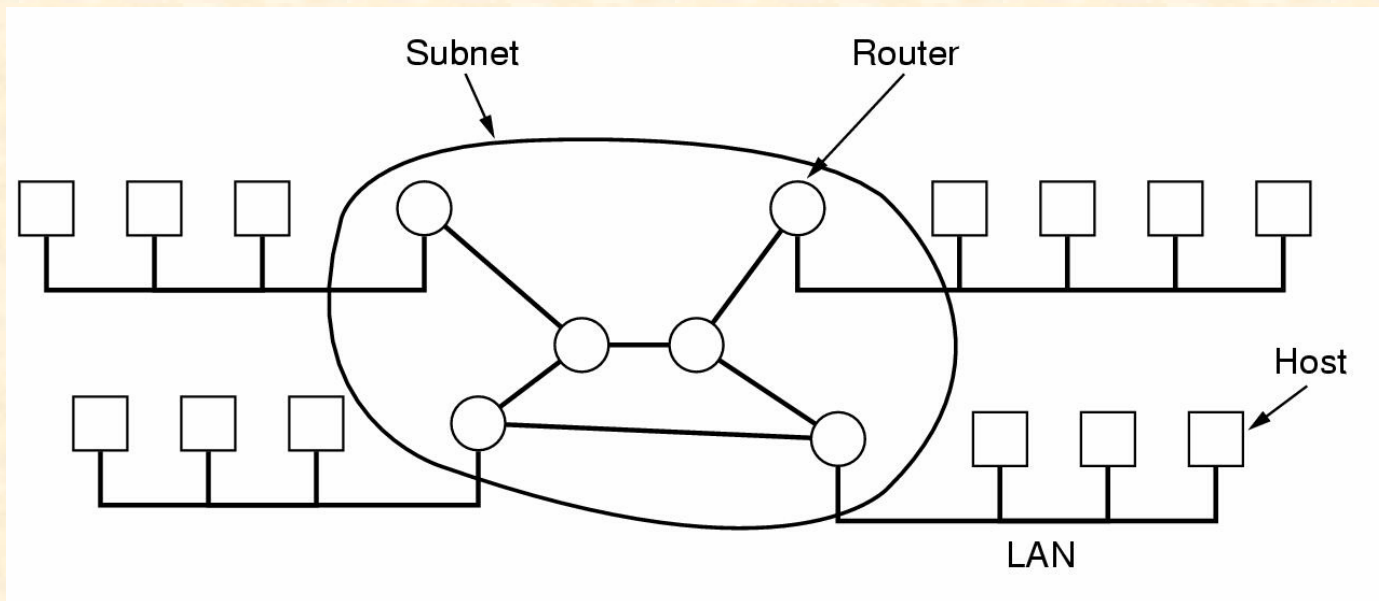
## ➤ Por escala

- **PAN: Redes de Área Personal**
  - Redes inalámbricas (bluetooth, NFC) en un radio de un metro.
- **LAN: Redes de Área Local**
  - Redes privadas dentro de un edificio o un terreno limitado (pueden ser varios kilómetros)
  - Suele estar implementadas como redes de difusión.
  - Suelen tener velocidades elevadas, pocos errores y bajo retardo.
  - Las topologías utilizadas suelen ser:
    - Bus: IEEE 802.3 Ethernet
    - Anillo: IEEE 802.5 Token Ring
- **MAN: Redes de Área Metropolitana**
  - Pueden ser públicas o privadas.
  - Existen como categoría al tener un estándar adaptada para ellas: IEEE 802.6 que consiste en dos buses unidireccionales a los que se conectan los equipos.

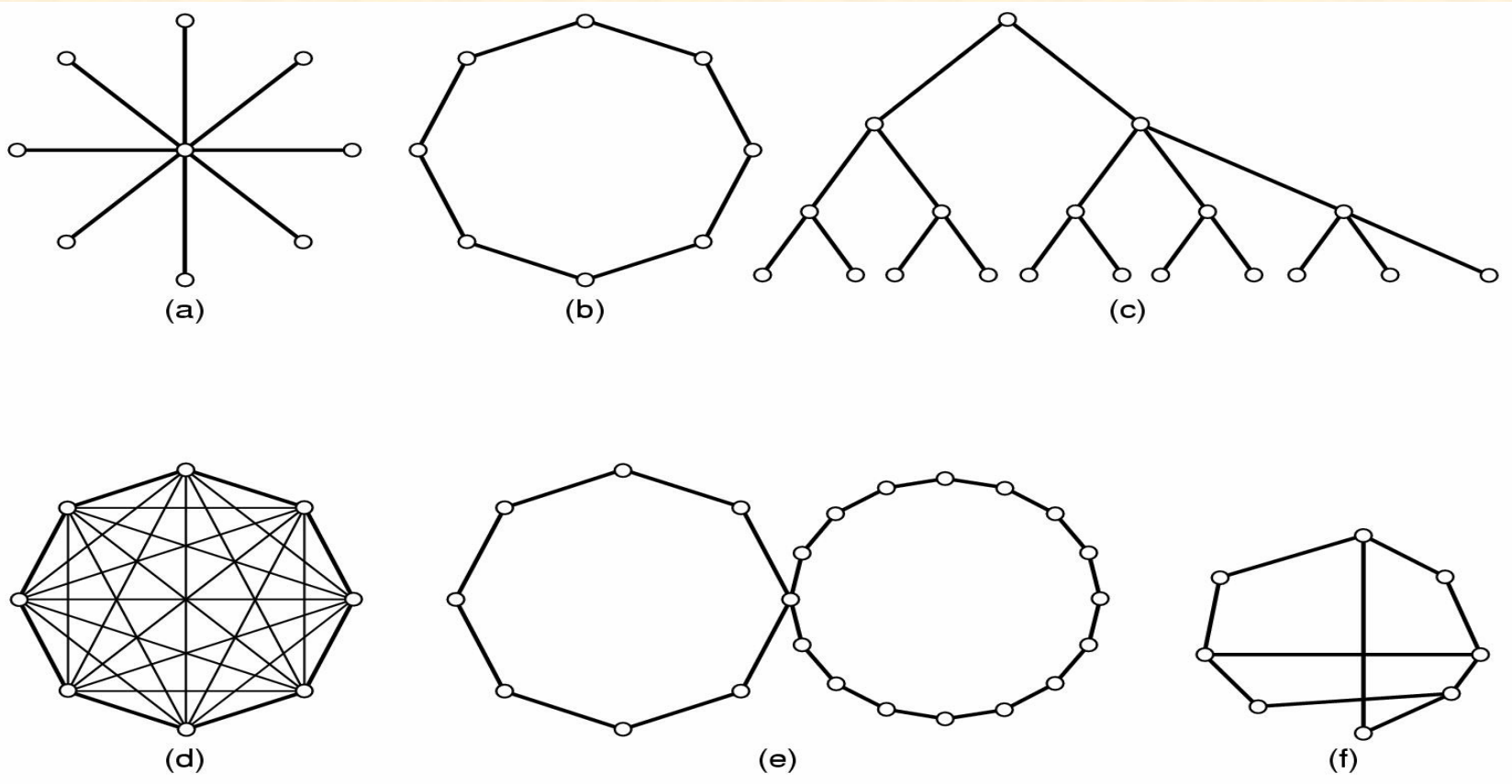




- **WAN: Redes de Área Extensa**
  - Redes que, a veces, pueden ocupar un país o un continente.
  - Están compuestas de:
    - **Hosts:** equipos de los usuarios
    - **Subred de comunicaciones:** elementos para conectar los hosts:
      - Líneas de transmisión
      - Elementos de conmutación (llamados encaminadores, enrutadores, routers, ...)



- **WAN: Redes de Área Extensa (Continuación)**
  - Los Routers de la subred de comunicaciones suelen utilizar conexión de punto a punto.
  - Existen varias topologías: a-Estrella, b-Anillo, c-Árbol, d-Malla, e-Intersección de anillos y f-Irregular







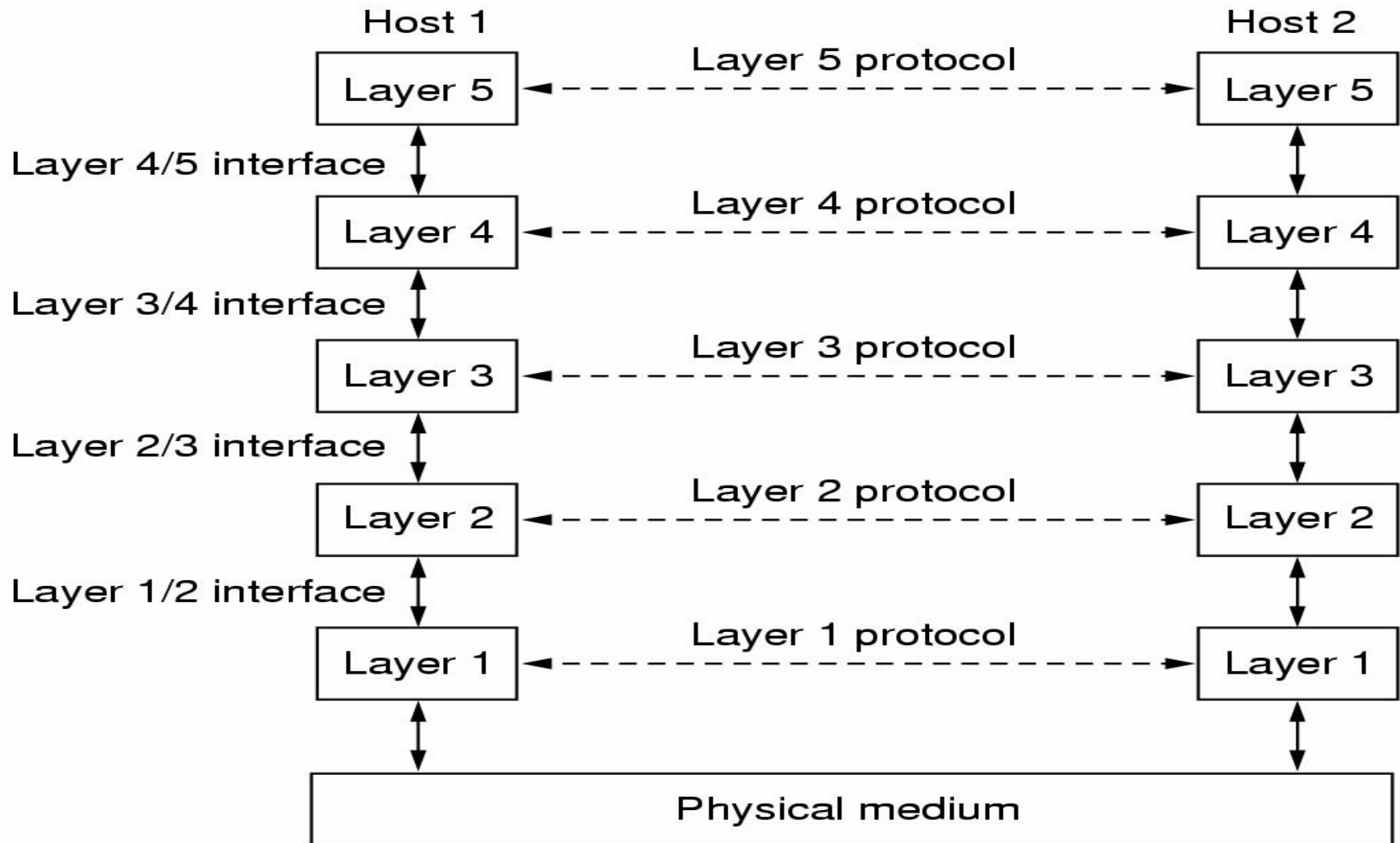
# Software de Red

# Jerarquía de Protocolos

## ➤ Capas

- Para reducir la complejidad del diseño las redes implementan una serie de capas o niveles
- Cada capa se encargará de unas tareas
- Entre el emisor y el receptor se establece un canal de comunicaciones a través del medio físico. Esta sería la capa más inferior y la única que, en realidad, transmite información entre los dos.
- Cada capa transmitirá la información a sus adyacentes sirviendo de capas de abstracción
- Sin embargo, cada capa deberá “hablar” con su homónima del otro lado siguiendo un lenguaje previamente establecido (protocolo)
- Esta “doble comunicación” se consigue haciendo que, en el emisor, una capa, al recibir la información de su capa superior añada cierta información que solo será entendida por su homónima del receptor, que se encargará de quitarla cuando reciba la información de su capa inferior. Este proceso se llama **encapsular**.
- El conjunto de capas y protocolos se denomina **Arquitectura de red**

- Un esquema de todo esto sería este:



- Un equivalente en la vida real:
  - Un filósofo, que habla inglés quiere transmitirle una información a un colega que está en otro lugar y que habla francés.
  - El filósofo le pasa la información a una traductora que sabe inglés y holandés y que sabe que en el otro lado un traductor entiende el holandés. Ésta, lo traduce y se lo pasa a la secretaria para que lo envíe.
  - En la secretaría reciben el mensaje y, como saben que en el destino hay un fax, le pone la información adecuada para saber a quien va enviado y la manda.
  - La secretaria de destino recibe la información, le quita la portada y se la da al traductor.
  - Éste, traduce al francés y se la pasa al destinatario final.

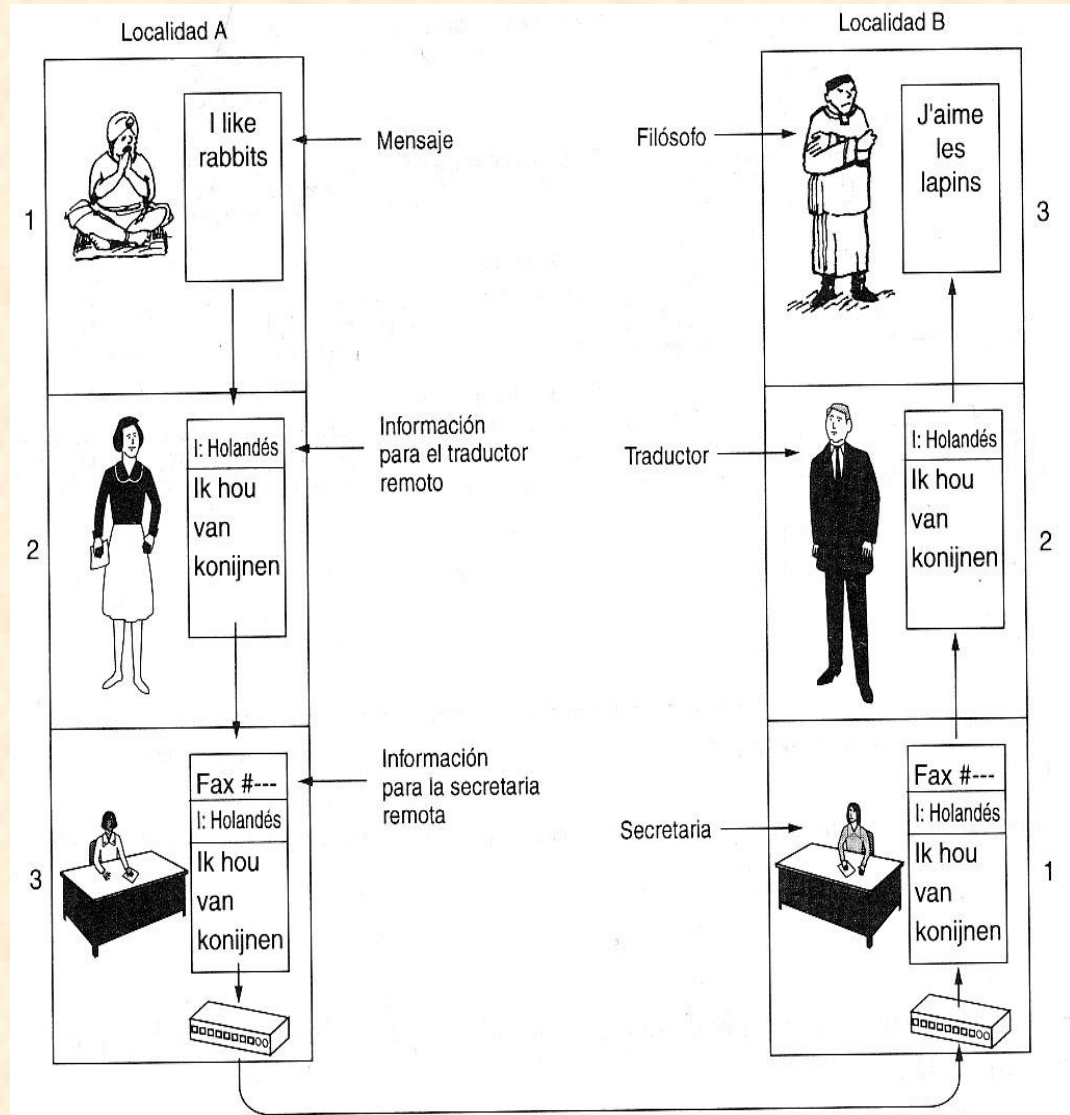
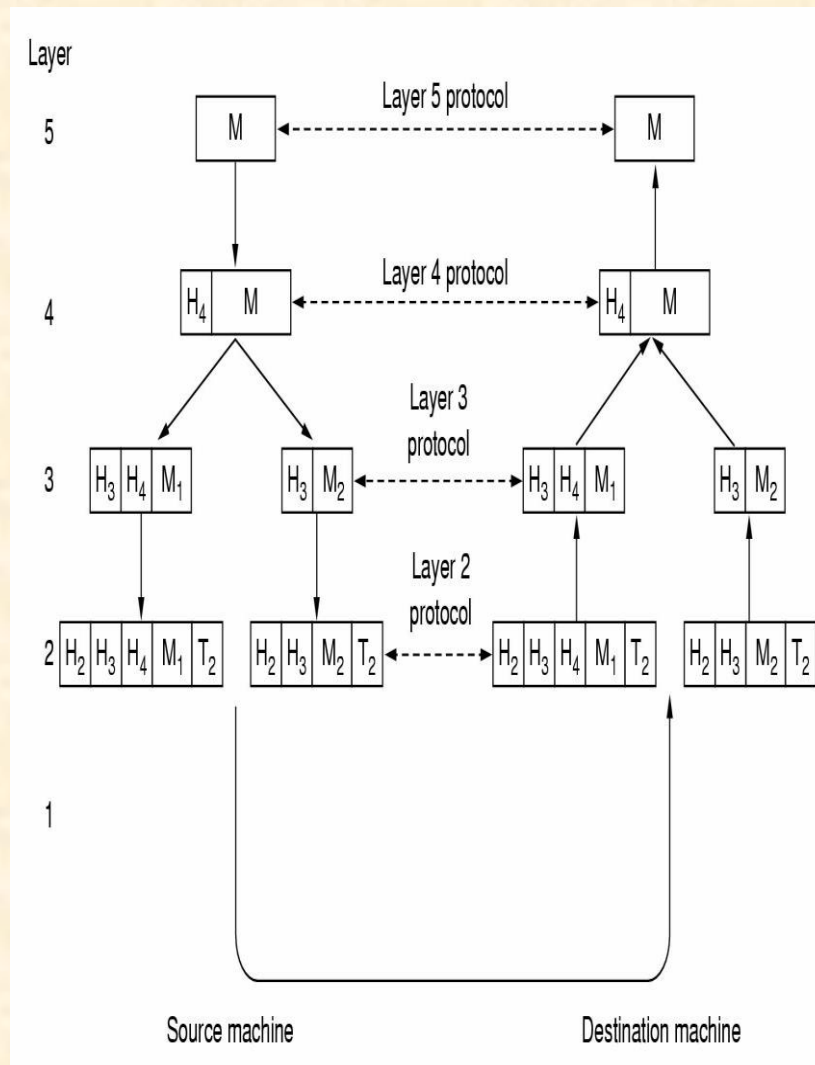



Figura 1-10. La arquitectura filósofo-traductor-secretaria.

- Y un ejemplo más técnico:

- Una aplicación situada en la capa 5 quiere enviar datos, en este caso una "M".
- Se la pasa a la capa 4 que le añade una cabecera para identificarlo y lo pasa a la capa 3. Esta nueva información la denominaremos **segmento**.
- La capa 3 trocea el segmento en unidades más pequeñas y le añade una nueva cabecera. Pasa cada trozo a la capa 2. Cada uno de los trozos lo denominaremos **paquete**.
- La capa 2 no solo añade una cabecera sino también un apéndice a cada uno de los paquetes entregando el resultado a la capa 1 para su transmisión física. A cada uno de estos bloques lo denominaremos **trama**.
- En la máquina destino, el mensaje se mueve hacia arriba de capa en capa eliminando la información añadida en el origen y recomponiendo el mensaje original.





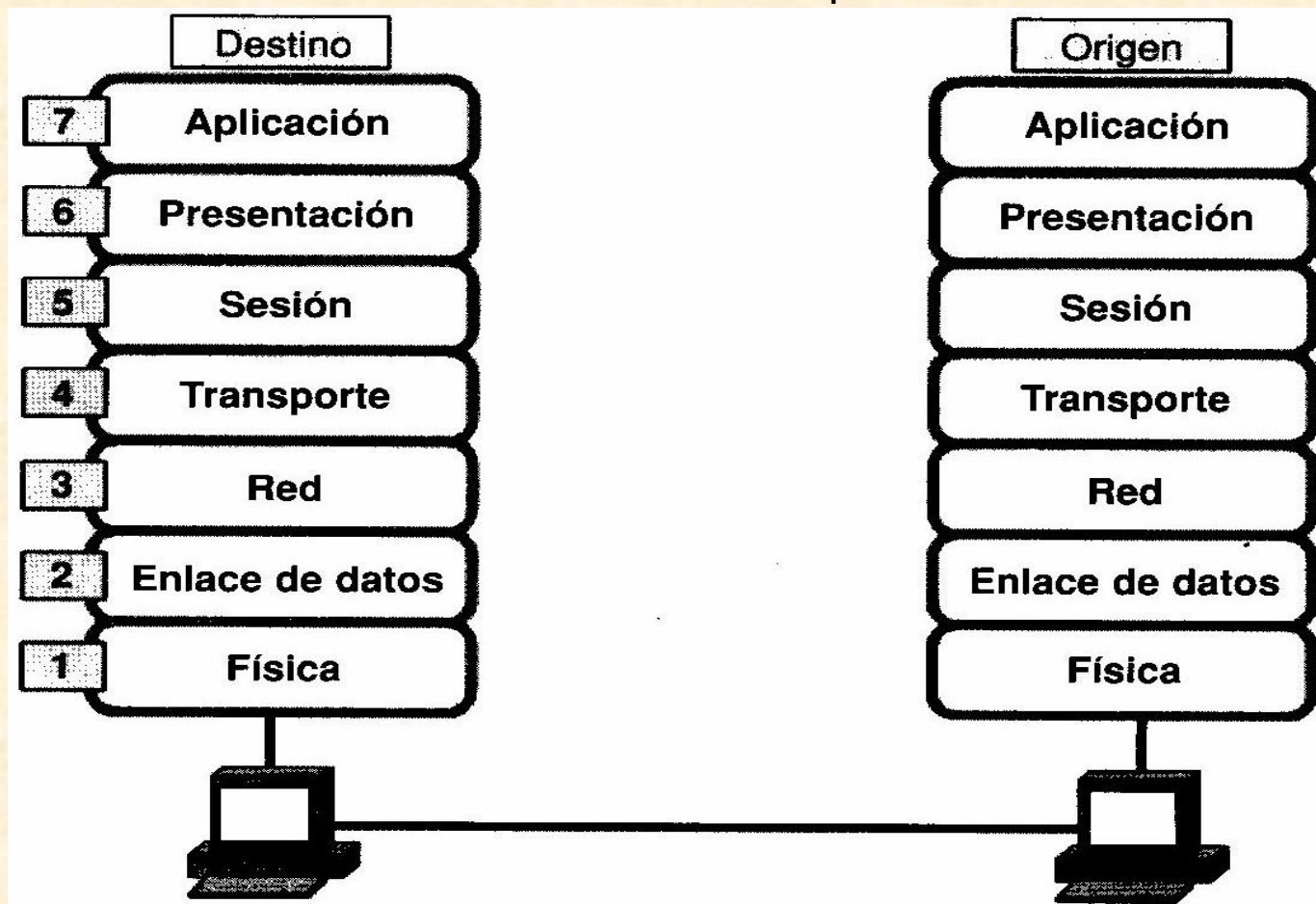
# Los Modelos de Referencia



# OSI (Open System Interconnection)

## ➤ Capas

- Modelo de referencia teórico en 7 capas



## ➤ Capa 1: Física

- Establece la forma de transmitir la información por el medio: Voltaje, duración, cables, conectores,...

## ➤ Capa 2: Enlace de datos

- Establecer una línea de comunicaciones libre de errores. Genera las **tramas** del tamaño adecuado al medio físico y creará las tramas de **acuse de recibo**.
- También se encarga del **control de flujo** (o **control de acceso al medio**).

## ➤ Capa 3: Red

- Permite la interconectividad entre equipos que se encuentren en redes geográficamente separadas.
- Establece los sistemas de **encaminamiento** entre redes.

## ➤ **Capa 4: Transporte**

- Trocea los datos para crear segmentos. El receptor se encargará de reordenarlos o pedir su retransmisión si es necesario.

## ➤ **Capa 5: Sesión**

- Establece, administra y finaliza sesiones de comunicación entre dos equipos.
- Gestiona la sincronización y el control de dialogo.

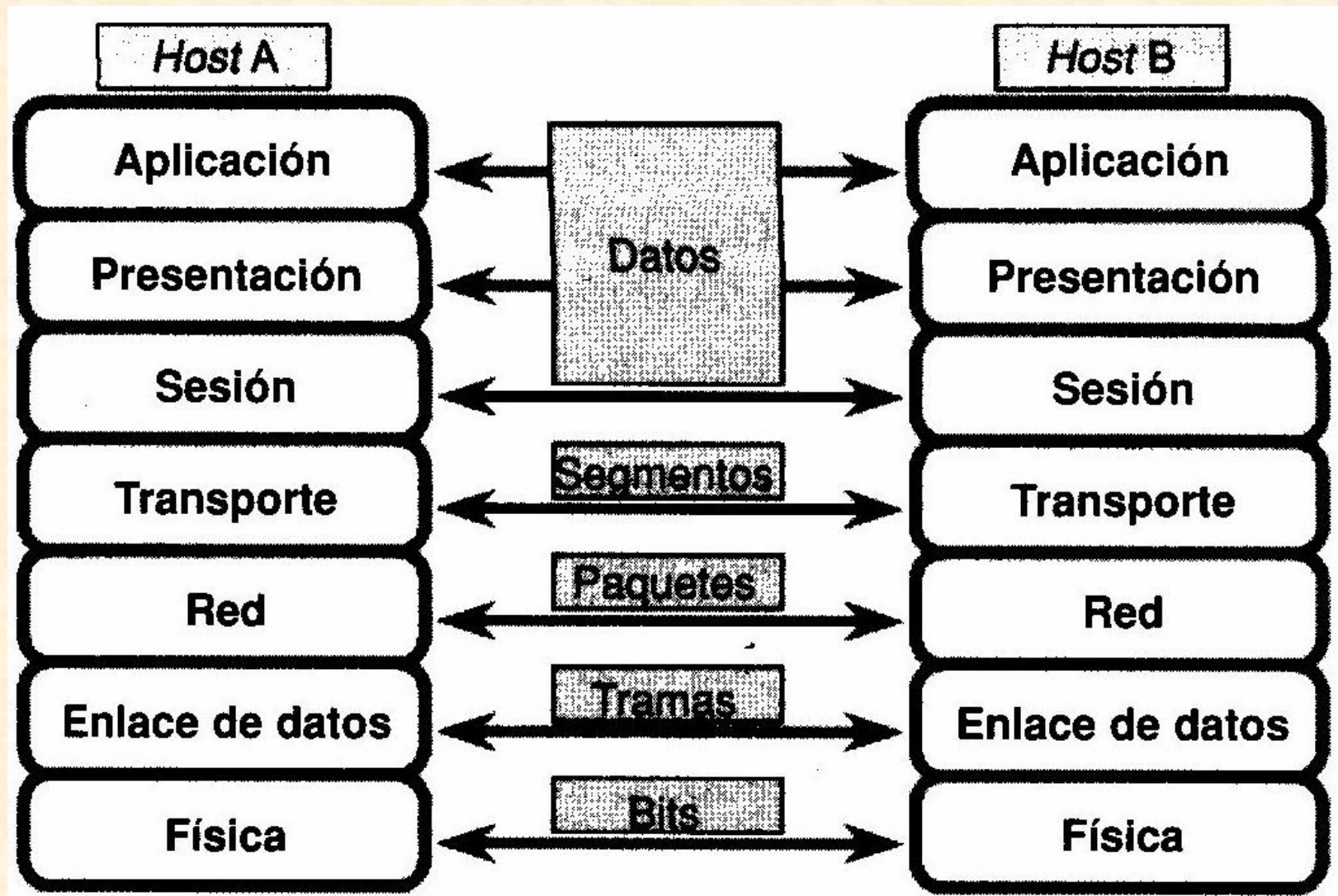
## ➤ **Capa 6: Presentación**

- Se asegura de que los datos serán entendidos por el receptor. Los traducirá, comprimirá o cifrará según sea necesario.

## ➤ **Capa 7: Aplicación**

- Proporciona servicios de red a las aplicaciones que las necesitan (acceso a datos, impresoras, ...)

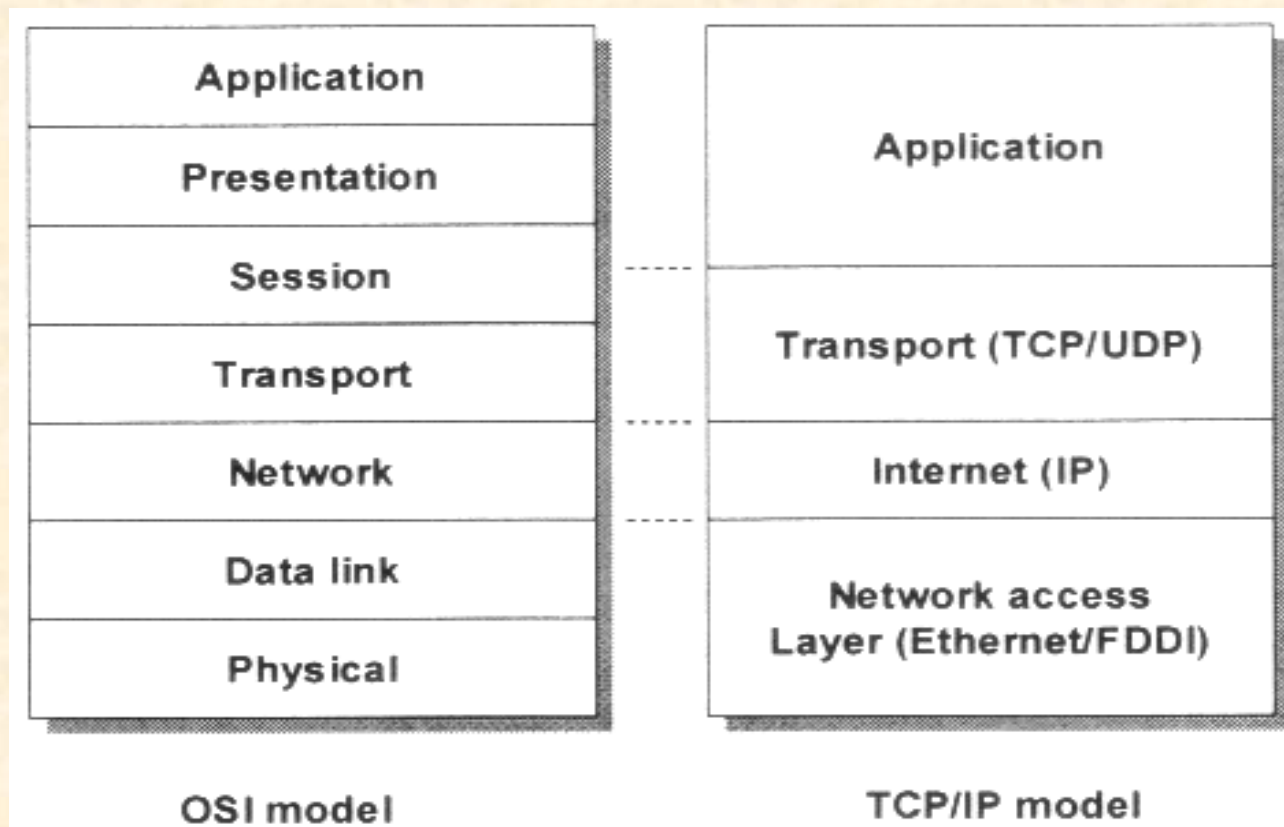
➤ Nombres de los datos en cada capa



# TCP/IP

## ➤ Capas

- Modelo de aplicación real en "4" capas (aunque realmente la capa de acceso a la red no está contemplada en el modelo)



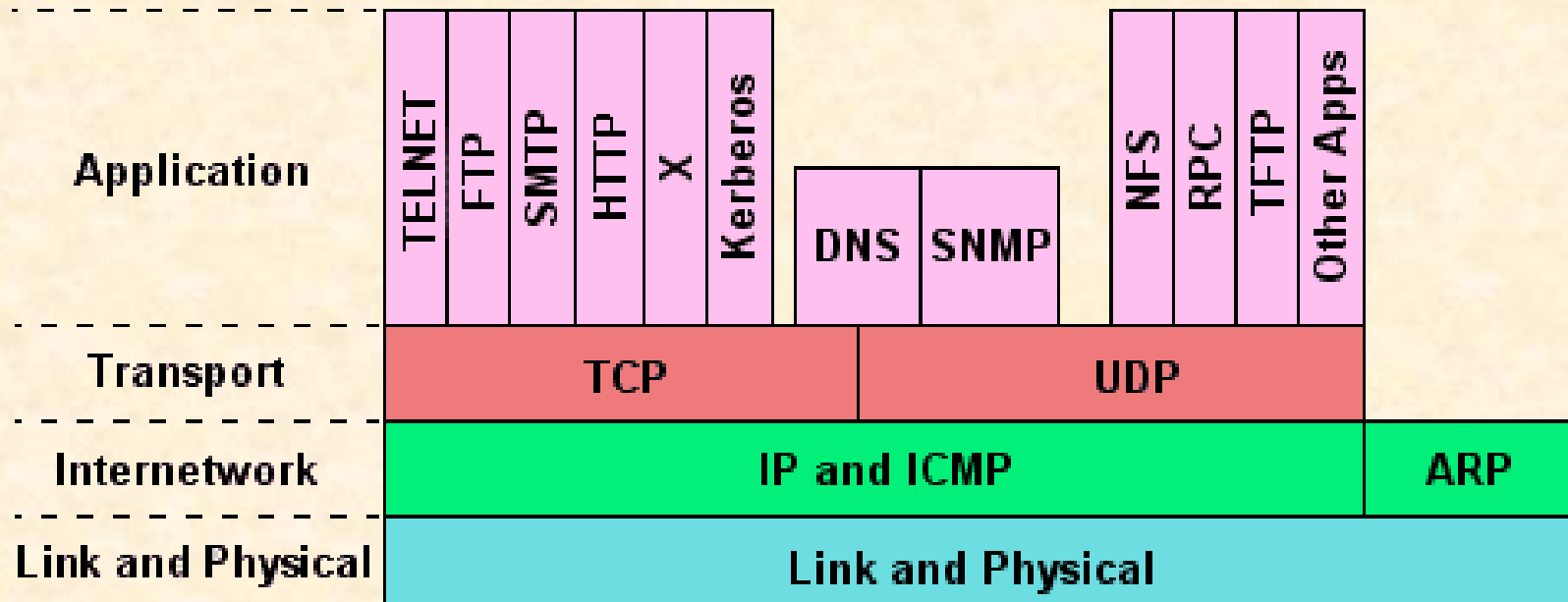


## ➤ Aplicaciones y protocolos en cada capa

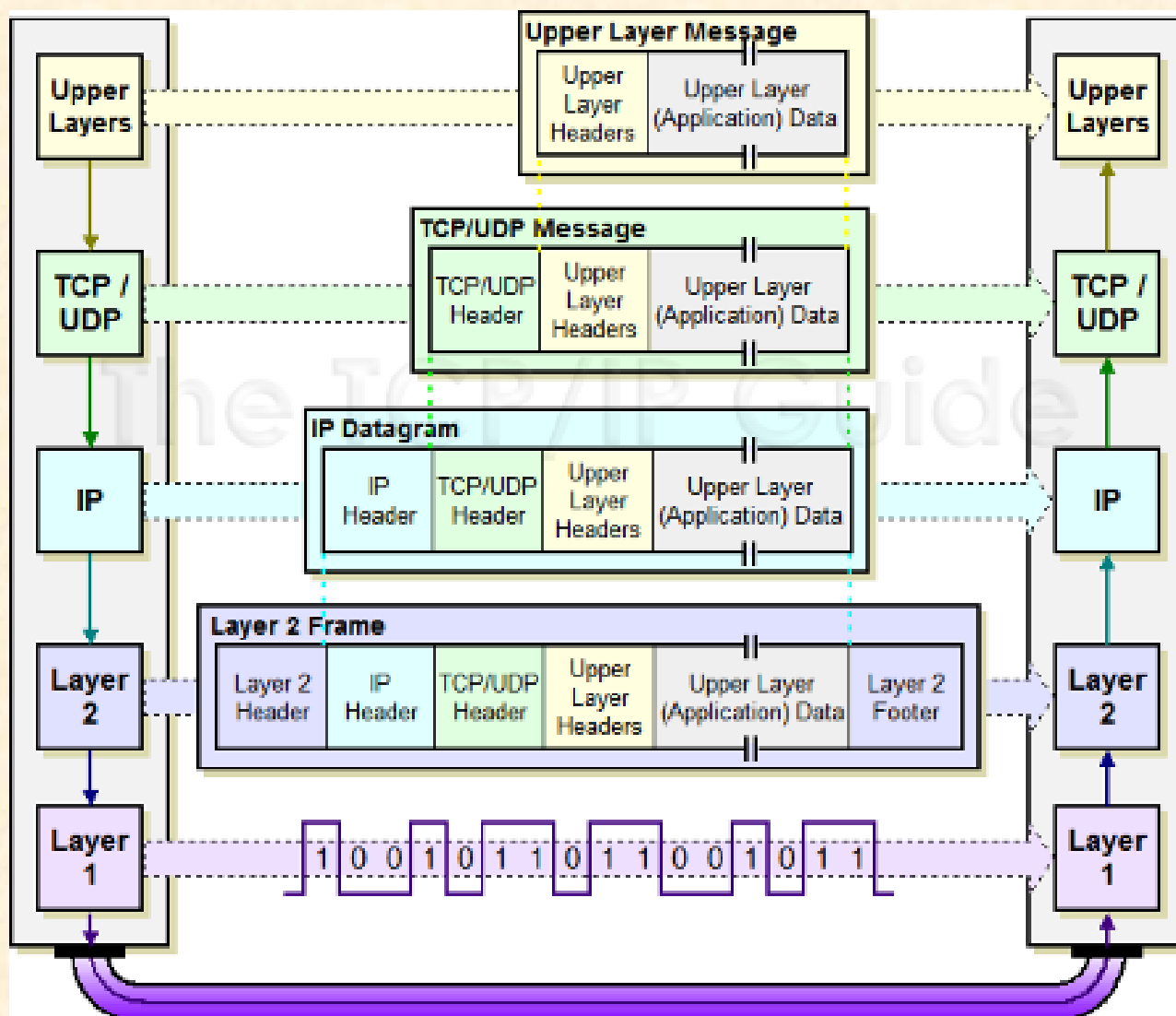
Application (Host To Host Layer)	Ping	Telnet & Rlogin		FTP	SMTP	SNMP	Trace-route		
	DNS	TFTP		BOOTP	RIP	OSPF	etc.		
Transport	TCP			UDP			ICMP		
Network	IP								
Data Link	LLC			HDLC			PPP		
	Ethernet	802.3	X.25	Token Ring		Frame Relay		ATM	SMDS
Physical	Fiber Optics		UTP	Coax	Microwave		Satellite		STP



## ➤ Protocolos de la capa de aplicación



## ➤ Cabeceras y pies





# Capa 1

# Física

# Medios de Transmisión

- Encargado de transmitir la información
- Ancho de Banda:
  - Cantidad de información que puede transmitirse por unidad de tiempo
  - Suele medirse en bps (bits por segundo)
  - Los múltiplos (Kbps, Mbps) utilizan potencias de 10
  - En medios analógicos no hay que confundir frecuencia con velocidad de transmisión: pueden transmitirse varios bits en cada onda.
- Dos tipos de medio:
  - **Guiados:** Existe un elemento físico que une los dos puntos (emisor y receptor). La información no puede salirse de ese camino
  - **No guiados:** Utilizan el aire o el espacio vacío para comunicar al emisor y al receptor

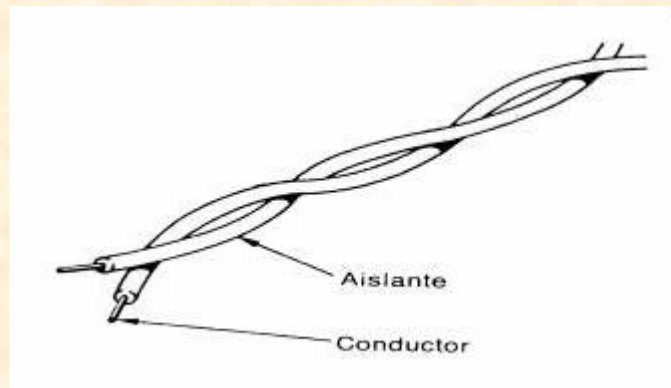
# Medios de Transmisión

## ➤ Medios Magnéticos

- No guiado
- No son estrictamente para comunicación de ordenadores en red, pero sirven para transmitir información entre emisor y receptor.
- Se trata de grabar la información en un soporte magnético (generalmente cintas) y transportarlas al destino.
- En determinados casos puede resultar el sistema más rápido para transmitir información.
- Podríamos incluir en este sistema a los medios no magnéticos como los ópticos y de estado sólido.

## ➤ Par trenzado

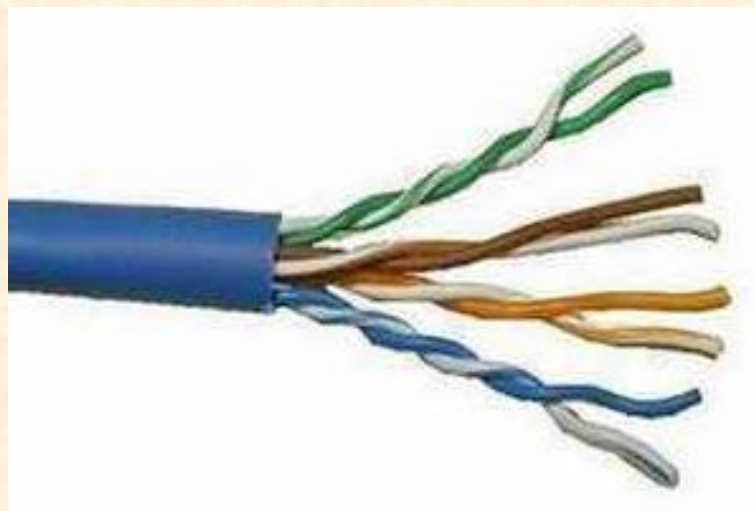
- Guiado
- La información se lanza como diferencia de potencial entre los dos cables del par.
- El trenzado sirve para que las interferencias electromagnéticas afecten a los dos hilos del par por igual.





## ➤ Par trenzado (continuación)

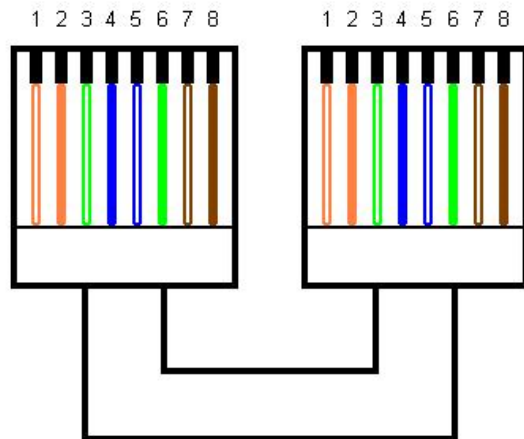
- Se suele utilizar un mazo con cuatro pares trenzados.
- Los cables pueden estar protegidos por una malla metálica (STP: Shielded Twisted Pair) o una hoja de aluminio (FTP: Foiled Twisted Pair) o no llevan protección alguna (UTP: Unshielded Twisted Pair)
- Los cables utilizados en LAN son UTP.
- Existen diferentes categorías (3, 5, 5e, 6). A mayor categoría mayor velocidad puede alcanzar la información transmitida. Esto se consigue aumentando el trenzado.
- Igualmente podemos encontrarlo como rígido o flexible.
  - Rígido: Alcanza más distancia, es más barato pero se rompe si se dobla demasiado o varias veces. Se utiliza para instalaciones fijas.
  - Flexible: Utilizado para latiguillos



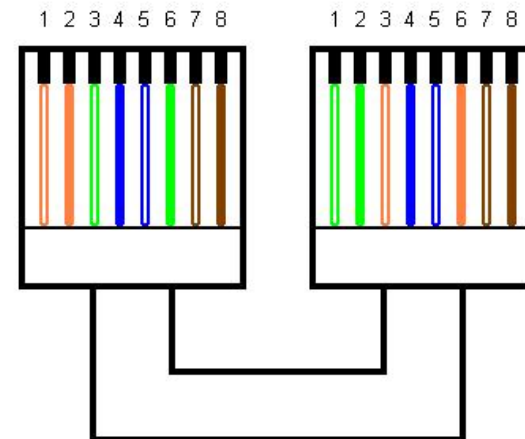
## ➤ Par trenzado (continuación)

- Para conectar equipos se utiliza un orden específico que permite alcanzar la máxima velocidad.
- Dependiendo del tipo de equipos que se conecten se utiliza la conexión estándar o la que se conoce como "cruzada"

EIA / TIA 568 B



Latiguillo cruzado



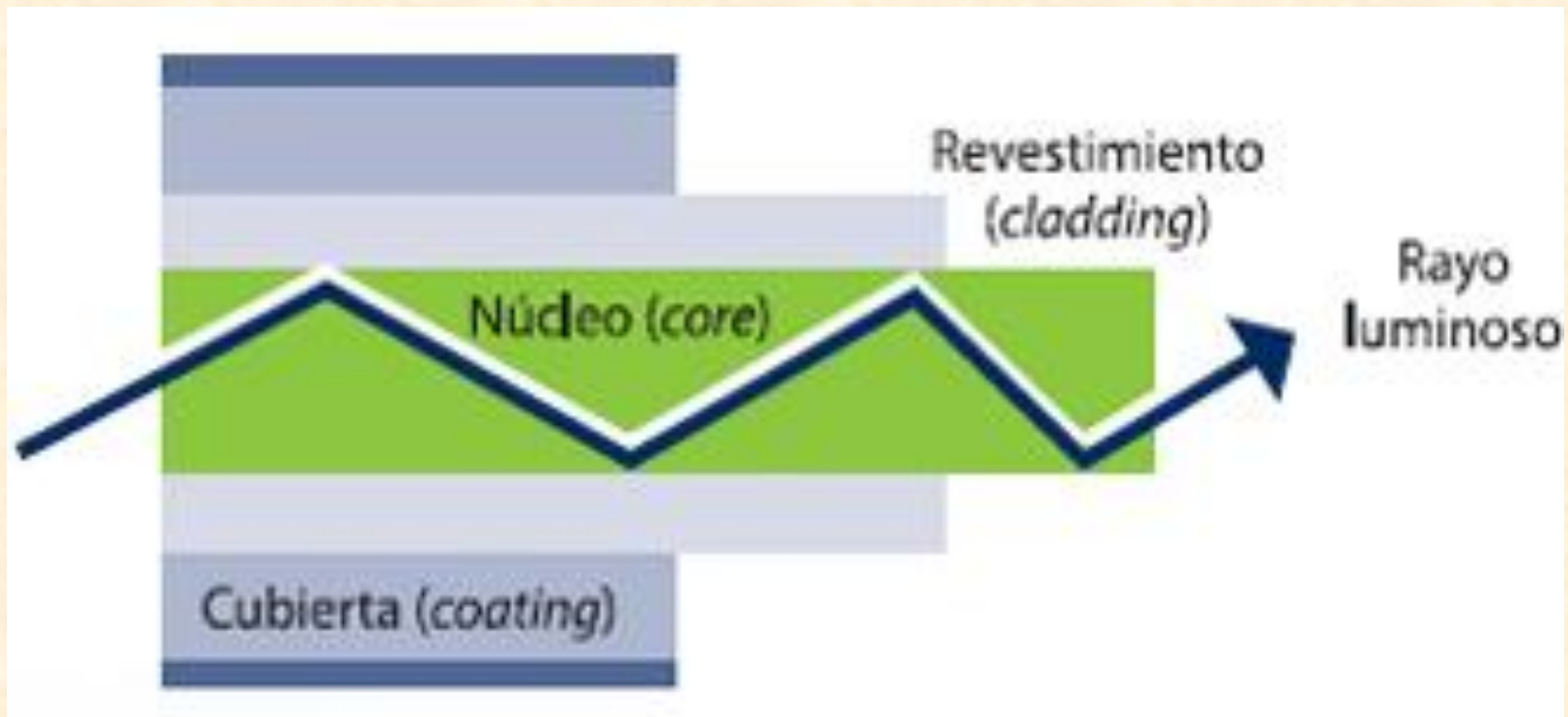
## ➤ Cable Coaxial

- Guiado
- Solo un cable se utiliza para transmitir la información
- Alrededor de este se sitúa una malla protectora que lo aísla de las interferencias externas
- Lo encontramos en dos versiones:
  - **Banda Base:** Transmisión de información digital. Poco utilizado en la actualidad
  - **Banda Ancha:** Transmisión de información analógica. Utilizado para transmisión de gran cantidad de información a largas distancias



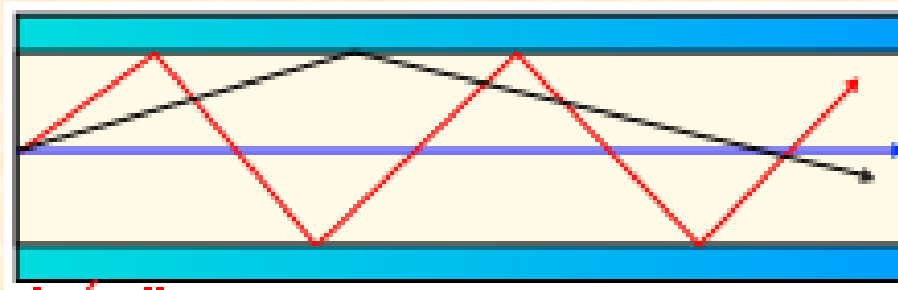
## ➤ Fibra óptica

- Guiado
- Hace uso de la propiedad de la luz cuando se produce un cambio de medio: se refracta, pero si llega con un determinado ángulo, se refleja.

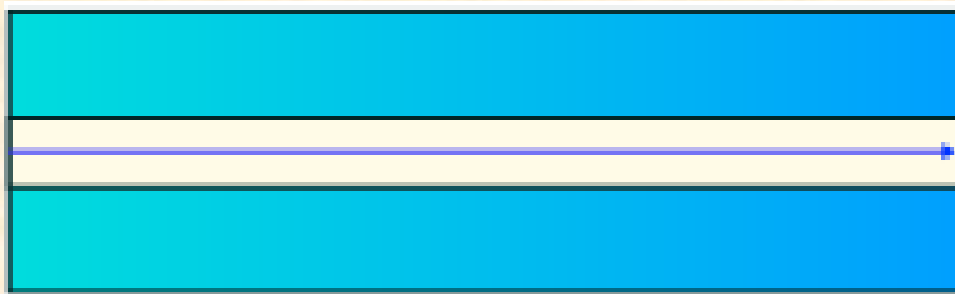


## ➤ Fibra óptica (continuación)

- Existen dos formas de utilización:
  - Multimodo
    - Cable más grueso
    - Permite utilizar más de un rayo por cable



- Monomodo
  - Cable más fino
  - Solo un rayo por cable
  - Alcanza mayores distancias y velocidad



## ➤ Transmisión inalámbrica

- No guiado
- Utiliza el aire o el vacío para transmitir
- Diferentes sistemas que emiten ondas de radio de diferentes frecuencias:
  - Radiotransmisión
  - Microondas
  - Satélite
  - Teléfono celular
- También pueden utilizarse ondas luminosas:
  - Infrarrojos
  - láser



## ➤ Wi-Fi

- Sistema de conexión de red de área local que no utiliza cable sino ondas de radio
- Existen varias versiones:
  - 11b: banda 2.4 GHz; 10Mbps
  - 11g: banda 2.4 GHz; 54Mbps
  - 11n: bandas 2.4 y 5 GHz; 600 Mbps (teóricamente)
  - 11ac: banda 5 GHz
- Las transmisiones pueden ir en abierto o codificadas según los sistemas de seguridad:
  - wep (versiones de 64 y 128 bits)
  - wpa (versiones 1 y 2)

## ➤ Elementos de conexión

- **Patch Panel:** Elemento físico al que se conectan los cables en un sistema de cableado estructurado
- **Transceptor:** Elemento físico al que se conecta el cable y sirve de enlace con el NIC (tarjeta de red)
- **Repetidor:** elemento electrónico que sirve para regenerar la señal
- **HUB:** repetidor multipuerto. Sirve para conectar múltiples equipos. La señal que le llegue por un puerto se repetirá por todos los demás. Pueden conectarse múltiples hubs en estrella o cascada. En cascada la comunicación entre los extremos será muy lenta o, incluso, podrá no llegar a producirse debido a las colisiones.



# Capa 2

## Enlace de Datos

# Introducción

## ➤ Factores a controlar en esta capa

- Los medios de transmisión no están exentos de errores
- La tasa de transferencia es finita
- Retardos entre envío y recepción

## ➤ Conceptos

- **Enmarcado:** Dividir el mensaje original en **tramas** (trozos de tamaño dado y conocido). Puede añadirse información de control de recepción (cabecera y cola) errores (información redundante). Otros nombres: frames, marcos.
- **Control de Errores:** Comprobar si la trama se ha recibido (acuse de recibo) o si es necesaria su retransmisión.
- **Control de Flujo:** Evitar que un transmisor rápido colapse a un receptor lento.

# Subcapas

- La capa se divide en dos subcapas con funciones diferentes
- **LLC: Control de enlace lógico**
  - Capa Superior (Cercana a la capa de red)
  - Encargada del control de flujo y detección de errores
- **MAC: Control de Acceso al Medio**
  - Capa inferior (cercana a la capa física)
  - Encargada de decidir quien puede transmitir en un momento dado

# Estandarización

## ➤ IEEE

- Instituto de Ingenieros Eléctricos y Electrónicos
- Se suele denominar IE-cubo
- Define estándares

## ➤ IEEE 802

- Estándares para la Capa de Enlace
- **802.1:** Define los estándares de la norma
- **802.2:** LLC
- **802.3, 802.4 y 802.5:** MAC
- **802.11:** Wi-Fi
- **802.15:** Bluetooth
- **802.16:** WiMax

# Subcapa LLC

## ➤ Detección y corrección de errores

- **Códigos de detección de errores:** Información redundante que permite detectar si la información recibida es correcta o no. Si no lo es se solicita su retransmisión
  - CRC (Código de Redundancia Cíclica)
  - Paridad
  - Checksum
- **Códigos de corrección de errores:** Información redundante que permite detectar si la información recibida es correcta o no. Si no lo es se intenta reconstruir la información original y, si no lo puede conseguir, se solicita su retransmisión.
  - Códigos de Hamming



## ➤ Control de Flujo

- Decidir cuantas tramas pueden mandarse simultáneamente
- Determinar cuales son las tramas que tienen que enviarse o reenviarse
- Algunos protocolos
  - Stop and Wait
  - Ventana Deslizante

# Subcapa MAC

## ➤ Función

- Establece los protocolos para que un equipo conectado a la red sea capaz de transmitir en un momento dado
- Existe un identificador único para cada adaptador de red denominado **Dirección MAC**
  - 48 bits (agrupados en 6 bloques de 2 dígitos hexadecimales)
  - Los 24 primeros representan al fabricante (un gran fabricante puede tener varios identificadores)

## ➤ Reparto del canal

- **Estático:** Tantas partes como equipos quieren transmitir. Cada uno de ellos solo tiene una parte del ancho de banda total
- **Dinámico:** Se reparte según las necesidades

## ➤ Conceptos

Vamos a suponer un escenario en el que hay un solo canal disponible para varios equipos que pueden transmitir en cualquier momento

- **Colisión:** Dos tramas coinciden en tiempo y espacio (de forma total o parcial). Ambas quedan destruidas
- **Tiempo continuo:** Un equipo puede transmitir una trama en cualquier momento
- **Tiempo ranurado:** El tiempo se divide en intervalos discretos (ranuras). Un equipo solo puede transmitir al principio de una ranura
- **Portadora:** Señal que lleva la información por el canal. Los equipos pueden detectarla para saber si el canal está libre o no.

## ➤ Protocolos sin detección de portadora

- **Aloha Puro:** Los equipos transmiten cuando lo consideran conveniente. Si se produce una colisión y la trama queda destruida se espera un tiempo aleatorio y se vuelve a transmitir
- **Aloha Ranurado:** Similar al anterior pero los equipos solo transmiten (o retransmiten) al comienzo de una ranura

## ➤ Protocolos con detección de portadora

- **Protocolos CSMA (Carrier Sense Multiple Access)**
  - **Persistente:** Cuando un equipo quiere transmitir observa el canal y se mantiene así hasta que deja de detectar una portadora. Si se produce una colisión, repite el proceso
  - **No Persistente:** Como el anterior pero si observa una portadora en el canal se retira un tiempo antes de comprobar de nuevo.
  - **CSMA/CD:** Si detecta que se produce una colisión corta inmediatamente la transmisión de la trama restante. Existe en modos persistente y no persistente

## ➤ Protocolos con detección de portadora (cont.)

- **Otros protocolos:**
  - **Libres de colisiones:** Por turnos
    - Mapa de bits,
    - Conteo descendente binario
  - **De contienda limitada:** Utilizar protocolos de contienda (aloha, csma, ...) cuando la carga es pequeña y libres de colisiones cuando la carga es alta.
    - Recorrido de árbol adaptable

# Estándares IEEE para subcapa MAC

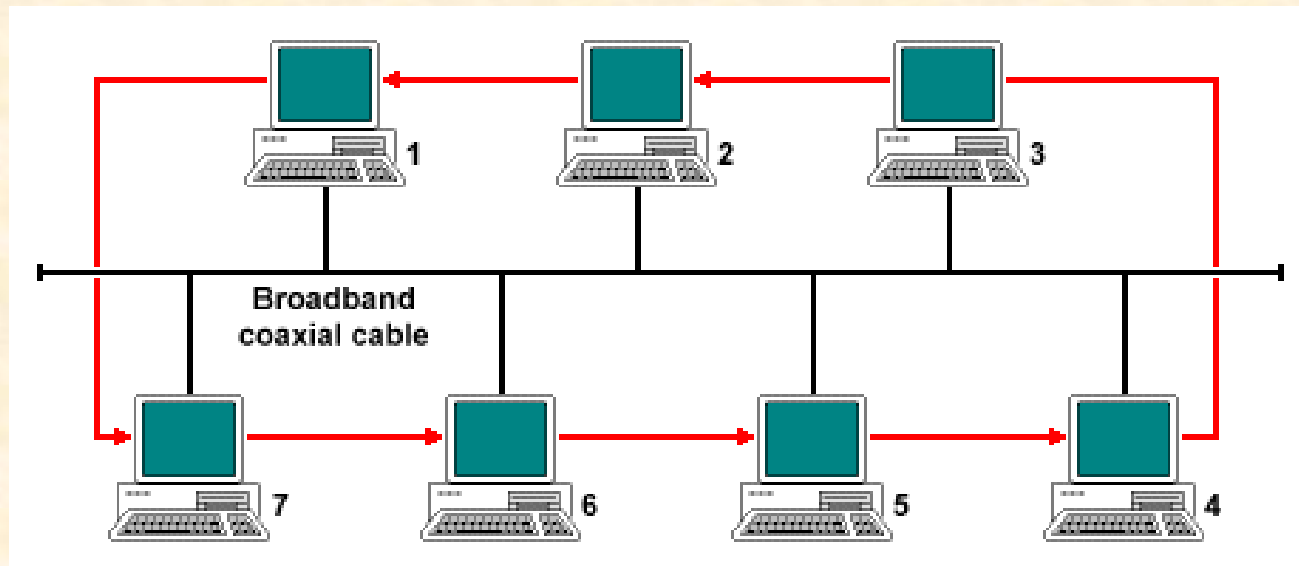
## ➤ 802.3 (Ethernet)

- Para LAN.
- Utiliza el protocolo CSMA-CD Persistente
- Cable coaxial:
  - 10Base5: Thick Ethernet
  - 10Base2: Thin Ethernet
- Par Trenzado
  - 10BaseT
  - 100BaseT: Fast Ethernet
  - 1000BaseT: Gigabit Ethernet
- Fibra óptica
  - 10BaseF
  - 100BaseF
  - 1000BaseF



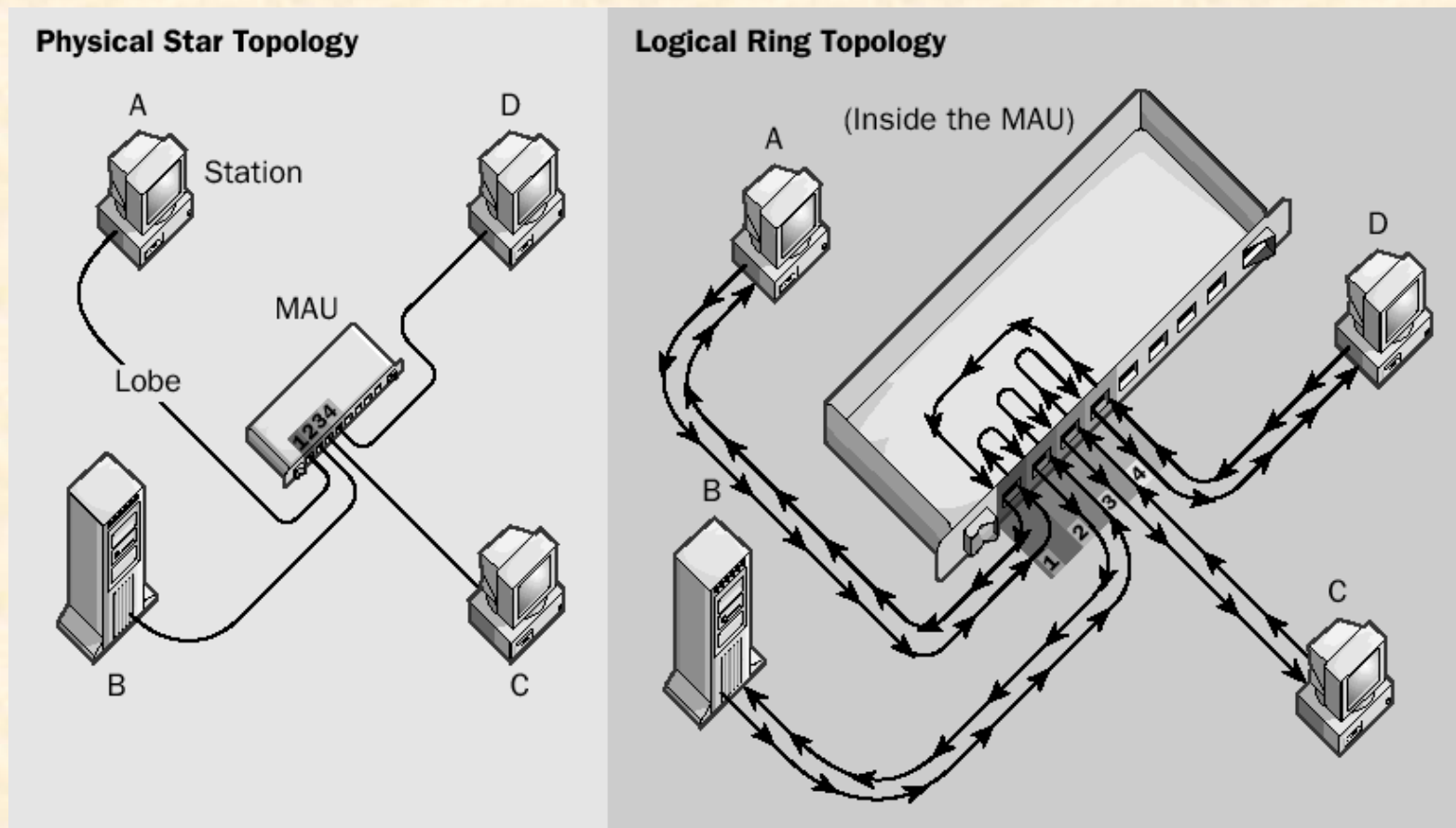
## ➤ 802.4 (Token Bus)

- Libre de colisiones
- Los equipos se conectan en bus pero se configuran como un anillo lógico
- Utiliza un sistema de fichas (token). Quien tiene la ficha, puede transmitir, pero solo la puede tener durante un tiempo limitado
- Uno de los equipos (cualquiera) debe encargarse del mantenimiento del anillo:
  - Mantenimiento de la ficha
  - Incorporación y eliminación de equipos en el anillo



## ➤ 802.5 (Token Ring)

- Similar a Token Bus pero algo más complejo
- Los equipos se conectan en estrella pero se configuran como un anillo lógico
- El elemento de conexión se denomina MAU (Media Attachment Unit)



## ➤ Elementos de conexión

- **NIC:** Network interface Controller. Elemento en el que se conecta el transceptor
- **Puente (Bridge):** Similar al repetidor. Guarda una tabla de los equipos que se encuentran en cada lado (su dirección MAC) y solo envía la información si el destinatario se encuentra allí. Para Esa tabla se rellena periódicamente por medio de Broadcasts
- **Switch:** Puente Multipuerto. Se utiliza para conectar HUB ya que disminuye drásticamente el tráfico en la red
- **Switch Gestionable:** Switch que permite la gestión de los puertos en estos aspectos:
  - Activar o desactivar los puertos
  - Monitorización
  - Agrupar los puertos en bloques lógicos: VLAN
  - Utilización de puertos comunes a diferentes VLAN (los NIC que se conecten a ellos deben poder ser configurados según el estándar 802.1q)



# Capa 3

## Red

# Funciones

- Se encarga de llevar los paquetes desde el origen hasta el destino
- El envío puede requerir saltos a través de dispositivos especiales
- Estos dispositivos pueden tener a su disposición diferentes caminos para llegar al destino
- Los dispositivos de la capa deben encontrar cual es el mejor camino para llegar al destino.
- Algunos algoritmos de enrutamiento:
  - **Estáticos:** Camino más corto, inundación
  - **Dinámicos:** Vector distancia, horizonte dividido

# Protocolo IP

- Protocolo de direccionamiento del modelo TCP/IP
- Actualmente coexisten las versiones 4 y 6.
  - **IPV4**: Direcciones de 32 bits (agrupadas en 4 bloques de 8 bits representados en base 10)
  - **IPV6**: Direcciones de 128 bits (agrupadas en 8 bloques de 16 bits representados en base 16)
- La versión 4 se encuentra saturada (desde hace años) y, aunque se han establecido una serie de mecanismos para alargar su vida se considera que está llegando al límite de su crecimiento. Aun así todavía se utilizará durante bastante tiempo
- La versión 6 está llamada a sustituir a la 4 y ya está implementada en todos los sistemas operativos modernos. En estos momentos todavía no se sabe cuando se realizará este cambio.

## ➤ Traducción de direcciones

- El protocolo IP permite identificar a los equipos origen y destino, pero los paquetes tienen que ser enviados a la capa de enlace para su transmisión
- Protocolos:
  - **ARP**: Busca la dirección MAC de un equipo del que se conoce su dirección IP
  - **RARP**: Un equipo que no tiene dirección IP difunde su MAC para ver si alguien es capaz de decirle cual es su dirección IP (la utilizan los equipos que no tienen disco en el momento de encenderse). RARP no se enruta
  - **BOOTP**: Como RARP pero enrutable



# Direcciones IPv4

- Identificador de 32 bits que se dividen en dos partes:
  - **Mayor peso:** Identificador de red. Un organismo es el encargado de asignar un identificador a la organización que lo solicita.
  - **Menor peso:** Identificador de host. Identifica a cada uno de los equipos de la red
- Se establecen una serie de clases en función del tamaño de las redes:

	← 32 Bits →			
Class				Range of host addresses
A	0	Network	Host	1.0.0.0 to 127.255.255.255
B	10	Network	Host	128.0.0.0 to 191.255.255.255
C	110	Network	Host	192.0.0.0 to 223.255.255.255
D	1110	Multicast address		224.0.0.0 to 239.255.255.255
E	11110	Reserved for future use		240.0.0.0 to 247.255.255.255

## ➤ Valores especiales

Id. Red	Id. Host	Uso
00...00	00...00	0.0.0.0 Usada solo en el arranque del equipo
11...11	11...11	255.255.255.255 Broadcast. Envío a todos los equipos conectados
Valor	00...00	Identificador de Red
Valor	11...11	Multicast: Envío a todos los equipos de la red
01111111	Valor	Generalmente 127.0.0.1 Dirección de retroalimentación (localhost)

Nota: **Valor** hace referencia a cualquier cadena de bits que no sea todo unos ni todo ceros

## ➤ NAT: Network Address Translation

- Sistema para **aumentar el ciclo de vida del protocolo IPV4**
- Multitud de redes en el mundo se configuran para acceder únicamente a los recursos internos de la red a la que pertenecen por lo que, en principio, puede haber dos o más equipos en el mundo que tengan la misma dirección IP.
- Si dos o más de esos equipos quiere conectarse a otras redes, los equipos que realizan el encaminamiento tendrán problemas para encontrar el camino de vuelta ya que no sabrán a cual de los equipos deberán ir.
- Para solucionarlo se establece un sistema por el que los equipos de esas redes internas puedan conectarse hacia el exterior pero que no sean accesibles, directamente, desde equipos de otras redes.

- Para ello, se establece un equipo que estará conectado a las redes mundiales y que podrá acceder y ser accedido desde cualquier red.
- Este equipo utilizará su dirección IP para navegar "en nombre" del equipo de la red interna. Esto es, "traduce" la dirección del equipo real por la suya, busca el recurso, establece una conexión y, cuando reciba las respuestas, se las enviará al equipo de la red interna que le haya hecho la solicitud
- Todos los equipos de esa red interna serán vistos desde los equipos de otras redes con el identificador del equipo que ha hecho el NAT lo que puede suponer un problema para el acceso a determinados recursos remotos:
  - Porque tengan limitado el numero de conexiones desde un cliente
  - Por baneos debidos a usos indebidos

- Para permitir una mejor organización de los equipos de conexión, se establecen una serie de redes reservadas para el propósito de ser utilizada en las redes internas. La RFC 1918 las denomina **Redes Privadas**
  - Clase A: 10.0.0.0
  - Clase B: 172.16.0.0 a 172.31.0.0
  - Clase C: 192.168.0.0 a 192.168.255.0
- Los equipos de encaminamiento pueden configurarse para que no realicen conexiones dirigidas a esas redes

## ➤ CIDR: Classless Inter-Domain Routing

- Las redes entregadas a las organizaciones, éstas las dividían según sus necesidades en redes más pequeñas (subredes).
- Para ello lo que se hace es "alargar" el identificador de red entregado tomando prestados bits de la parte del identificador de host. Para saber a que subred pertenece un equipo no es suficiente con saber la clase. hay que indicar cuantos bits se utilizan para identificarla.
- El tamaño del identificador de subred se indica por medio de un valor conocido como **máscara de subred**.
- Dado que las organizaciones no necesitaban la mayor parte de las subredes que podían generar, la organización IANA (la encargada de repartir las redes) las recuperó para repartirlas a otras organizaciones. Esto ha permitido alargar, aun más, la vida del protocolo IPV4.



- Estas organizaciones y no reciben una red completa sino parte de ella. Para esto se le asigna la subred acompañada del número de bits que la fijan.
- Así pues, las clases, como tales, ya no sirven para identificar a las redes y los equipos de encaminamiento han debido adaptarse a esta situación (Classless)
- Cada organización podrá gestionar su subred de la forma que considere conveniente (como, por ejemplo, creando nuevas subredes)
- Con la llegada de CIDR la máscara de subred se suele identificar con número de bits en lugar de con un conjunto de 4 bloques en base 10 que era la forma tradicional



## ➤ Máscara de Subred

- La máscara de subred es un valor en binario que tiene cierta cantidad de unos contiguos en los bits de mayor peso y ceros en el resto. p.e.

1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0
---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---

- En algunos casos se considera la clase para establecer un valor “por defecto” de la máscara:
  - Clase A: 8 bits
  - Clase B: 16 Bits
  - Clase C: 24 Bits

## ➤ Representación de la máscara de subred

- Una forma es como en la dirección IP: agrupando en 4 bloques de 8 bits pasados a base 10
- Solo pueden tener estos valores:

0	0	0	0	0	0	0	0	0
1	0	0	0	0	0	0	0	128
1	1	0	0	0	0	0	0	192
1	1	1	0	0	0	0	0	224
1	1	1	1	0	0	0	0	240
1	1	1	1	1	0	0	0	248
1	1	1	1	1	1	0	0	252
1	1	1	1	1	1	1	0	254
1	1	1	1	1	1	1	1	255

- Los valores “todo ceros” y “todo unos” son los más habituales
- Así, la máscara de la página anterior (24 bits) se representaría:  
255.255.255.0

- Con la llegada de CIDR se suele utilizar la longitud de la máscara en lugar de los cuatro bloques en base 10. Así,
  - Un equipo con estos datos:  
Dirección IP: 192.168.1.1  
Máscara de subred: 255.255.255.0  
  
se representaría como  
192.168.1.1/24
- Para identificar a las redes, ya que no hay clases, se haría lo mismo:
  - Las redes de Clase A y Clase C  
87.0.0.0  
218.114.1.0  
  
se representarían como  
87.0.0.0/8  
218.114.1.0/24
  - En este caso, también nos encontraremos con el concepto "prefijo de red" que representa a los bits fijados como identificador de la subred sobreentendiendo que el resto, son ceros. Por ejemplo:
    - 87/8
    - 218.114.1/24
- El sistema de Prefijo de red es el utilizado para representar a las redes en IPV6

## ➤ Identificador de Subred

- Cuando se conoce la dirección IP y la máscara de subred de un equipo el identificador de subred se calcula haciendo un **y lógico** entre ambas

0	1	0	1	0	1	0	0	0	1	0	1	0	1	0	1	0	0	1	1	1	1	1	1	0	IP: 84.85.74.126
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	Máscara: 255.255.192.0 (18)
0	1	0	1	0	1	0	0	0	1	0	1	0	1	0	1	0	0	0	0	0	0	0	0	0	Id. Subred: 84.85.64.0

- En el identificador de subred se puede apreciar que:
  - los bits de la dirección IP que coinciden con 1 en la máscara, quedan igual
  - los bits de la dirección IP que coinciden con 0 en la máscara, quedan a 0
- Dos equipos se encuentran en la misma subred cuando coincide su identificador de subred

## ➤ Identificador de Subred (cont.)

- Si trabajamos en base 10 no es necesario convertir toda la dirección, ya que hay que tener los siguientes aspectos:
  - 255 = 11111111: Ese bloque quedará igual que en la IP
  - 0 = 00000000: Ese bloque quedará a cero.
  - Al menos tres de los bloques de la máscara son 255 o 0
- Por tanto, es necesario hacer operaciones en uno como máximo

195	194	25	47	IP: Base 10
255	255	255	0	Mascara: Base 10
195	194	25	0	Id Subred: Base 10

84	85	74	126	IP: Base 10
		0 1 0 0 1 0 1 0		IP: Base 2
255	255	192	0	Mascara: Base 10
		1 1 0 0 0 0 0 0		Máscara: Base 2
		0 1 0 0 0 0 0 0		Id Subred: Base 2
84	85	64	0	Id Subred: Base 10

# Subredes

- Una vez asignada una subred (a la que a partir de ahora llamaremos, simplemente, la red), esta puede subdividirse por el simple método de "tomar prestados" bits del identificador de host.
- Se tomarán prestados los bits de mayor peso que se necesiten y se unirán a la máscara de subred asignada originalmente.
- Por ejemplo, partiendo de una máscara de 24 bits, si tomamos prestados 3:

1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0
---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---

Nueva máscara de subred: 27 bits

255.255.255.224

- Dependiendo de los sistemas de conexión utilizados pueden ser inutilizables las subredes que tienen todo ceros o todo unos en los bits prestados
  - Todo ceros: el identificador de esa subred coincide con el de la red
  - Todo unos: la dirección de broadcast de esa subred coincide con la de la red



## ➤ Creación de subredes del mismo tamaño

- Se pueden crear  $2^n$  subredes. Siendo  $n$  el número de bits prestados
- Vamos a suponer, a partir de ahora, que podemos utilizar las dos subredes problemáticas. Si no fuese así tendríamos que restar la o las prohibidas.
- Si lo que conocemos es el numero de subredes a crear ( $S$ ),  $n$  se calcula de la siguiente manera
$$n \geq (\log S / \log 2)$$



## ➤ Creación de subredes del mismo tamaño (cont.)

- El número de hosts que puede contener cada subred es  $2^h - 2$

Siendo h el número de bits que hemos dejado para el identificador de host (los que quedan a 0 en la máscara)

- Esto es debido a que no puede haber un host numerado con todo ceros (coincidiría con el identificador de subred) ni uno con todo unos (se utiliza para multicast en la subred)
- Se dice que una subred está optimizada cuando se utilizan todas las direcciones posibles para hosts
- Hay que tener cuidado con equipos que necesitan IP dentro de una subred como impresoras y routers
- Las subredes diseñadas de esta manera no pueden ampliarse

## ➤ Creación de subredes del mismo tamaño (cont.)

- Ejemplo

Nos dan la red 84.85.0.0/16 y queremos hacer 6 subredes:  
El identificador de la red en binario es:

0	1	0	1	0	1	0	0	0	1	0	1	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---

Calculamos el numero de bits que hemos de tomar prestados  
 $n \geq (\log 6 / \log 2) \rightarrow n \geq 3$

Los identificadores de las seis subredes serán:

0	1	0	1	0	1	0	0	0	1	0	1	0	1	0	1	0	0	0	0	0	0	0	0	S0: 84.85.0.0/19
0	1	0	1	0	1	0	0	0	1	0	1	0	1	0	1	0	0	1	0	0	0	0	0	S1: 84.85.32.0/19
0	1	0	1	0	1	0	0	0	1	0	1	0	1	0	1	0	1	0	0	0	0	0	0	S2: 84.85.64.0/19
0	1	0	1	0	1	0	0	0	1	0	1	0	1	0	1	0	1	1	0	0	0	0	0	S3: 84.85.96.0/19
0	1	0	1	0	1	0	0	0	1	0	1	0	1	0	1	1	0	0	0	0	0	0	0	S4: 84.85.128.0/19
0	1	0	1	0	1	0	0	0	1	0	1	0	1	0	1	1	0	1	0	0	0	0	0	S5: 84.85.140.0/19

Si lo preferimos en decimal, la máscara de subred sería  
255.255.224.0

## ➤ Creación de subredes del mismo tamaño (cont.)

Ahora tendremos que numerar los hosts dentro de cada subred. Así, si numeramos, por ejemplo, los de la S2, las direcciones válidas serán:

01010100	01010101	01000000	00000001	84.85.64.1/19
01010100	01010101	01000000	00000010	84.85.64.2/19
				...
01010100	01010101	01000000	11111111	84.85.64.255/19
01010100	01010101	01000001	00000000	84.85.65.0/19
				...
01010100	01010101	01011111	11111101	84.85.95.253/19
01010100	01010101	01011111	11111110	84.85.95.254/19

Así podemos ver que la dirección de multicast de la subred será

01010100	01010101	01011111	11111111	84.85.95.255
----------	----------	----------	----------	--------------

## ➤ VLSM. Variable Length Subnet Masking

- Subredes de distinto tamaño
- Cuando tenemos subredes creadas cada una de ellas puede ser tratada como una red para crear nuevas subredes en ella sin que sea necesario hacerlo en el resto
- De esta forma nos encontraremos con subredes que toman prestados diferente número de bits
- Por ejemplo, Creamos dos subredes y, sobre la segunda, creamos cuatro iguales:

Subred A	Subred B	Subred C	Subred D	Subred E
----------	----------	----------	----------	----------

- La subred A toma prestado 1 bit. Ese bit tendrá valor 0
- Para el resto de subredes ese bit tendrá valor 1
- Ahora tomamos prestados otros dos que tendrán valores 00, 01, 10 y 11
- Juntándolos al bit que teníamos antes esas subredes tomarán prestados 3 bits sobre la red original y sus valores serán, pues 100, 101, 110 y 11

## ➤ Creación de subredes de distinto tamaño (cont.)

- P.E. Si realizamos esa operación sobre la red 192.168.1.0/24
- Tomamos un bit prestado para crear dos subredes iguales:

Subred A	Subred B
192.168.1. <b>0</b> 0000000/25	192.168.1. <b>1</b> 0000000/25

- Ahora tomamos otros dos en la subred b para crear las cuatro subredes

Subred A	Subred B1	Subred B2	Subred B3	Subred B4
	<b>1</b> 0000000	<b>1</b> 0100000	<b>1</b> 1000000	<b>1</b> 1100000

- Los identificadores de las subredes serán, pues:
  - Subred A: 192.168.1.0/25
  - Subred B1: 192.168.1.128/27
  - Subred B2: 192.168.1.160/27
  - Subred B3: 192.168.1.192/27
  - Subred B4: 192.168.1.224/27



## ➤ Creación de subredes de distinto tamaño (cont.)

- Esta operación la podemos realizar las veces que queramos en las subredes que deseemos
- P.E. Sobre la red 192.168.1.0/24
- Tomamos un bit prestado para crear dos subredes iguales:

Subred A <b>192.168.1.00000000/25</b>	Subred B <b>192.168.1.10000000/25</b>
--	--

- Ahora tomamos otro en la subred B para crear dos subredes

Subred A	Subred B1 <b>10000000</b>	Subred B2 <b>11000000</b>
----------	------------------------------	------------------------------

- Y por último tomamos otro en la subred B2 para crear otras dos subredes

Subred A	Subred B1	Subred B21 <b>11000000</b>	Subred B22 <b>11100000</b>
----------	-----------	-------------------------------	-------------------------------

- Los identificadores de las subredes serán, pues
  - Subred A: 192.168.1.0/25
  - Subred B1: 192.168.1.128/26
  - Subred B21: 192.168.1.192/27
  - Subred B22: 192.168.1.224/27

# Supernetting

## ➤ Suma de redes

- Identificador de red que engloba a varias subredes o equipos
- Se toma la parte común de mayor peso de las subredes o equipos que se quieran sumar. Los bits de menor peso restantes se dejarán a cero
- La máscara será la que ocupe esa parte común.
- P.E.

11000000	10101000	01000110	00000000	192.168.70.0/24
11000000	10101000	01010000	00000000	192.168.80.0/24
11000000	10101000	01011010	00000000	192.168.90.0/24
11000000	10101000	01000000	00000000	Parte Común
11111111	11111111	11100000	00000000	Máscara
11000000	10101000	01000000	00000000	192.168.64.0/19

- Ojo
  - La superred puede agrupar equipos o redes que no deseemos incluir. Si ese es el caso no podrá utilizarse. En su lugar habrá que calcular varias superredes que engloben lo deseado sin hacerlo con lo no deseado



## ➤ Suma de redes (cont.)

- Si añadimos otra red:

11000000	10101000	00010100	00000000	192.168.20.0/24
11000000	10101000	01000110	00000000	192.168.70.0/24
11000000	10101000	01010000	00000000	192.168.80.0/24
11000000	10101000	01011010	00000000	192.168.90.0/24
11000000	10101000	00000000	00000000	Parte Común
11111111	11111111	10000000	00000000	Máscara
11000000	10101000	00000000	00000000	192.168.0.0/17

## ➤ Suma de redes (cont.)

- La máscara puede ser menos restrictiva si lo deseamos

11000000	10101000	00010100	00000000	192.168.20.0/24
11000000	10101000	01000110	00000000	192.168.70.0/24
11000000	10101000	01010000	00000000	192.168.80.0/24
11000000	10101000	01011010	00000000	192.168.90.0/24
11000000	10101000	00000000	00000000	Parte Común
11111111	11111111	00000000	00000000	Máscara
11000000	10101000	00000000	00000000	192.168.0.0/16

## ➤ Suma de redes (cont.)

- Si trabajamos con bloques de 8 bits no es necesario utilizar el binario

10	2	15	0	/24
10	2	21	0	/24
10	2			Parte Común
10	2	0	0	/16

10	1	1	0	/24
10	2	0	0	/16
10				Parte Común
10	0	0	0	/8

## ➤ Agrupación estricta

- Agrupar equipos o redes sin incluir ninguno fuera de los deseados
- Para hacerlo hay que mirar no solo los bits que son iguales sino aquellos que los diferencian de los no deseados.
- La máscara de subred debe incluir el primer bit diferente de los no deseados
- P.E. Para agrupar a los equipos del rango 192.168.1.50 - 192.168.1.59

192.168.1.49	1	1	0	0	0	0	0	0	1	0	1	0	1	0	0	0	0	0	0	0	0	0	1	0	0	1	1	0	0	0	1		
192.168.1.50	1	1	0	0	0	0	0	0	1	0	1	0	1	0	0	0	0	0	0	0	0	0	1	0	0	1	1	0	0	1	0	192.168.1.50/31	
192.168.1.51	1	1	0	0	0	0	0	0	1	0	1	0	1	0	0	0	0	0	0	0	0	1	0	0	1	1	0	0	1	1			
192.168.1.52	1	1	0	0	0	0	0	0	1	0	1	0	1	0	0	0	0	0	0	0	0	1	0	0	1	1	0	1	0	0			
192.168.1.53	1	1	0	0	0	0	0	0	1	0	1	0	1	0	0	0	0	0	0	0	0	1	0	0	1	1	0	1	0	1	192.168.1.52/30		
192.168.1.54	1	1	0	0	0	0	0	0	1	0	1	0	1	0	0	0	0	0	0	0	0	1	0	0	1	1	0	1	1	0			
192.168.1.55	1	1	0	0	0	0	0	0	1	0	1	0	1	0	0	0	0	0	0	0	0	1	0	0	1	1	0	1	1	1			
192.168.1.56	1	1	0	0	0	0	0	0	1	0	1	0	1	0	0	0	0	0	0	0	0	1	0	0	1	1	1	0	0	0	192.168.1.56/30		
192.168.1.57	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	1	0	0	1	1	1	0	0		1	
192.168.1.58	1	1	0	0	0	0	0	0	1	0	1	0	1	0	0	0	0	0	0	0	0	1	0	0	1	1	1	0	1	0			
192.168.1.59	1	1	0	0	0	0	0	0	1	0	1	0	1	0	0	0	0	0	0	0	0	1	0	0	1	1	1	0	1	1			
192.168.1.60	1	1	0	0	0	0	0	0	1	0	1	0	1	0	0	0	0	0	0	0	0	1	0	0	1	1	1	1	0	0			

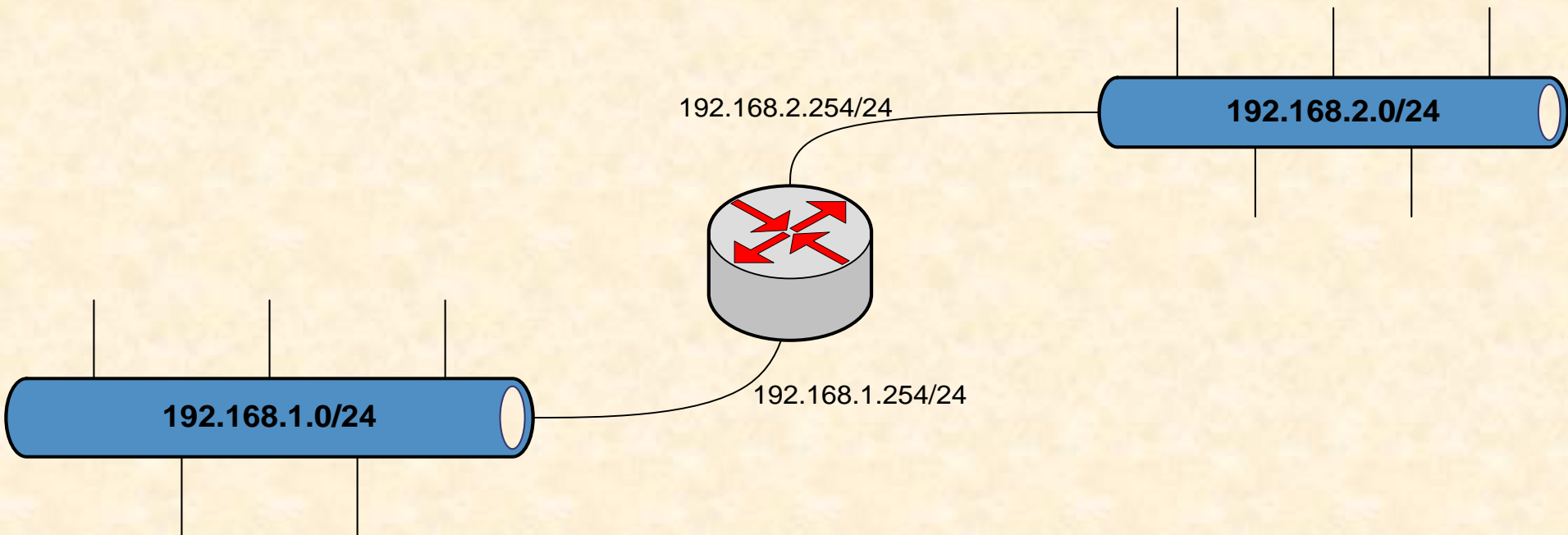
- Si tomásemos los bits que son iguales para el rango deseado (28 bits) se observa que también se incluyen los equipos anteriores y posteriores
- En cada extremo se tiene que encontrar cual es el primer bit diferente y llegar hasta el (en el extremo superior 31 bits y en el inferior 30 bits)
- Una vez calculadas las subredes que agrupan los extremos sin pasarse, se calculan las subredes de los equipos del interior que falten

# Dispositivos de conexión

## ➤ Router

- Enrutador, encaminador, puerta de enlace, gateway
- Equipo que conecta dos o más subredes
- Tiene dos o más interfaces de red
- Cada interface puede tener una o más direcciones IP
- Filtra el tráfico (no enruta los broadcast producidos ni por los equipos de capa2 ni por los equipos de capa3 salvo que se configure expresamente alguno de ellos)

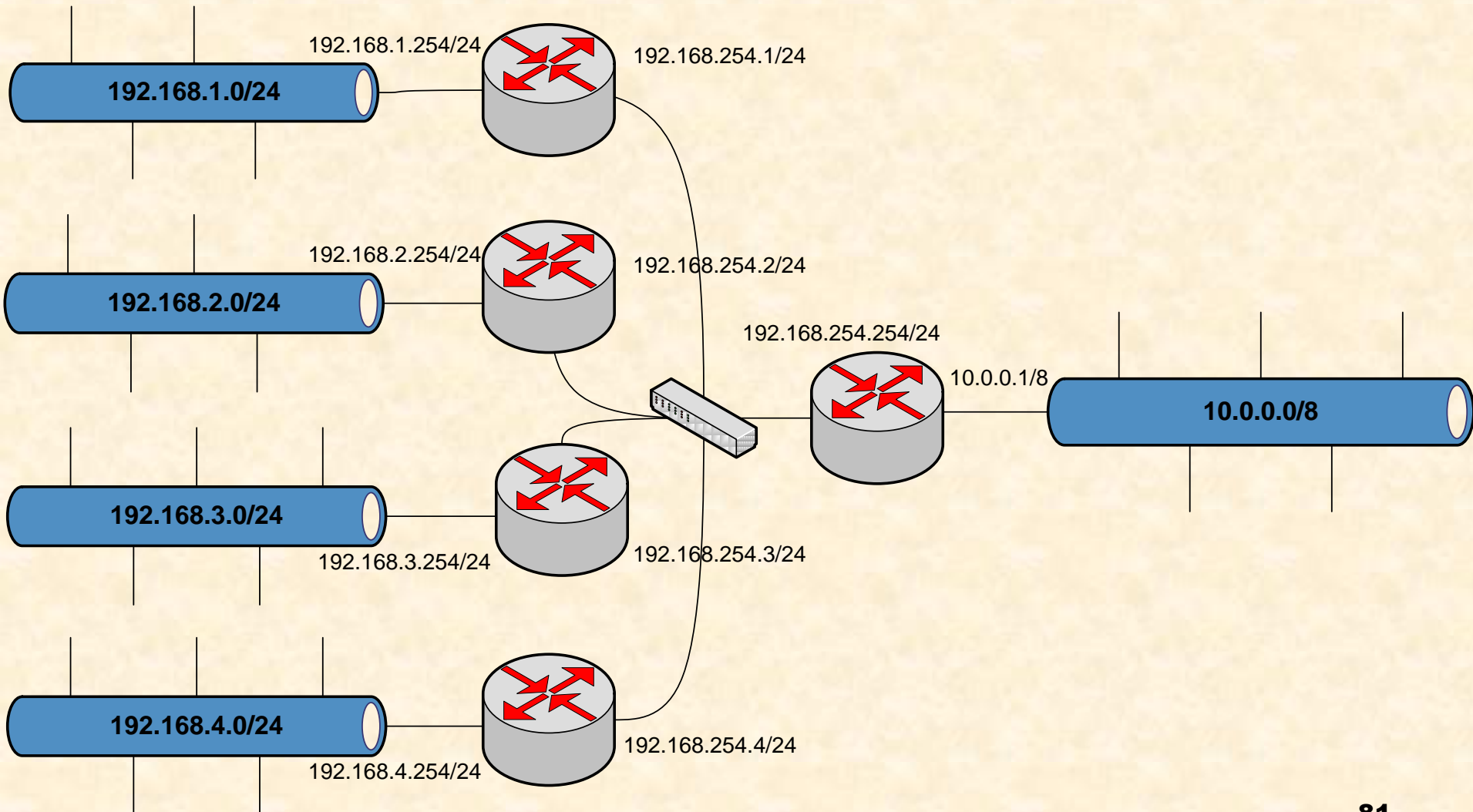
## ➤ Conexión de dos subredes





## ➤ Conexión de tres o más subredes

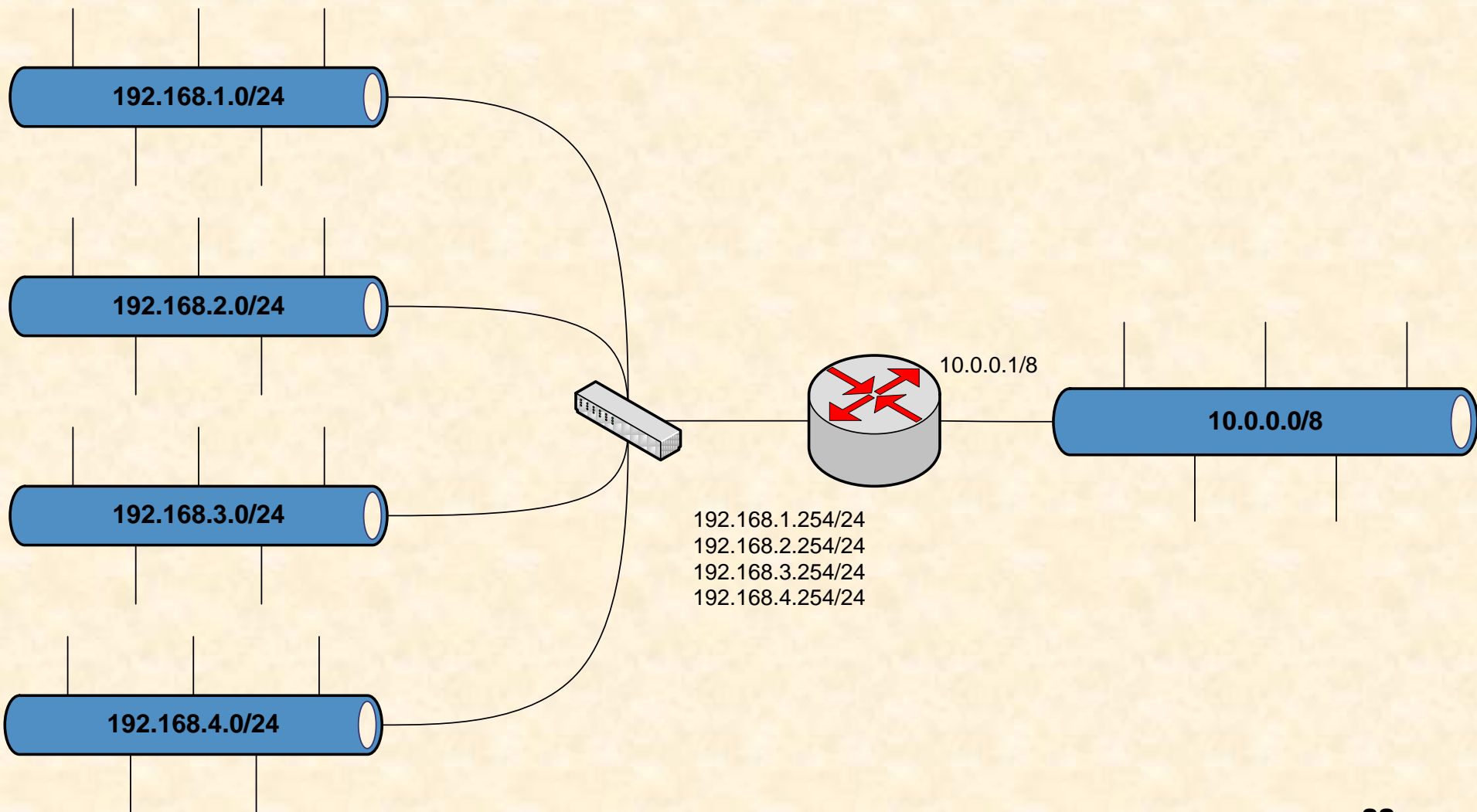
- routers con una IP por adaptador





## ➤ Conexión de tres o más subredes

- Router con múltiples IP



# Conexión de una LAN privada a Internet

## ➤ IP Pública

- Solo los equipos que tienen una IP que no se encuentre en los rangos de IP privadas pueden conectarse a través de los enrutadores de internet
- Las LAN suelen tener direcciones IP privadas para poder comunicarse entre si y utilizan un router que soporte NAT para poder conectarse con el exterior
- Todas las conexiones son realizadas por el router en nombre de los equipos de la LAN
- Si el router no es lo suficientemente potente puede alcanzarse el número máximo de conexiones que puede soportar con facilidad
  - Si esto ocurre no podrán establecerse nuevas conexiones y los equipos de la LAN notarán que no pueden "salir" a internet
- Los equipos de la LAN podrán establecer conexiones hacia el exterior a través del NAT pero desde el exterior no se podrán comunicar directamente con los equipos.
  - Al tener que conectarse directamente al router éste actúa como cortafuegos impidiendo que puedan producirse ataques directos a los equipos
  - Si algún equipo de la LAN va a dar un servicio que deba ser accedido directamente desde el exterior deberán configurarse reenvíos desde el router hacia las aplicaciones (hablaremos de ellos en la capa 7)

## ➤ **Modo Puente (Bridge)**

- En este modo un router no actúa como NAT sino que pasa la dirección IP Pública a otro equipo
- Este equipo estará conectado directamente al exterior por lo que podrá dar servicios pero también se verá afectado directamente por los posibles ataques que se produzcan
  - Deberá tener un sistema de cortafuegos potente
- Si otros equipos de la LAN quieren acceder a internet podrán hacerlo a través de él si soporta la "conexión compartida a internet"
- En muchos casos se configura el modo puente en los routers proporcionados por los ISP para conectar al otro lado un router más potente que de más posibilidades de configuración y control

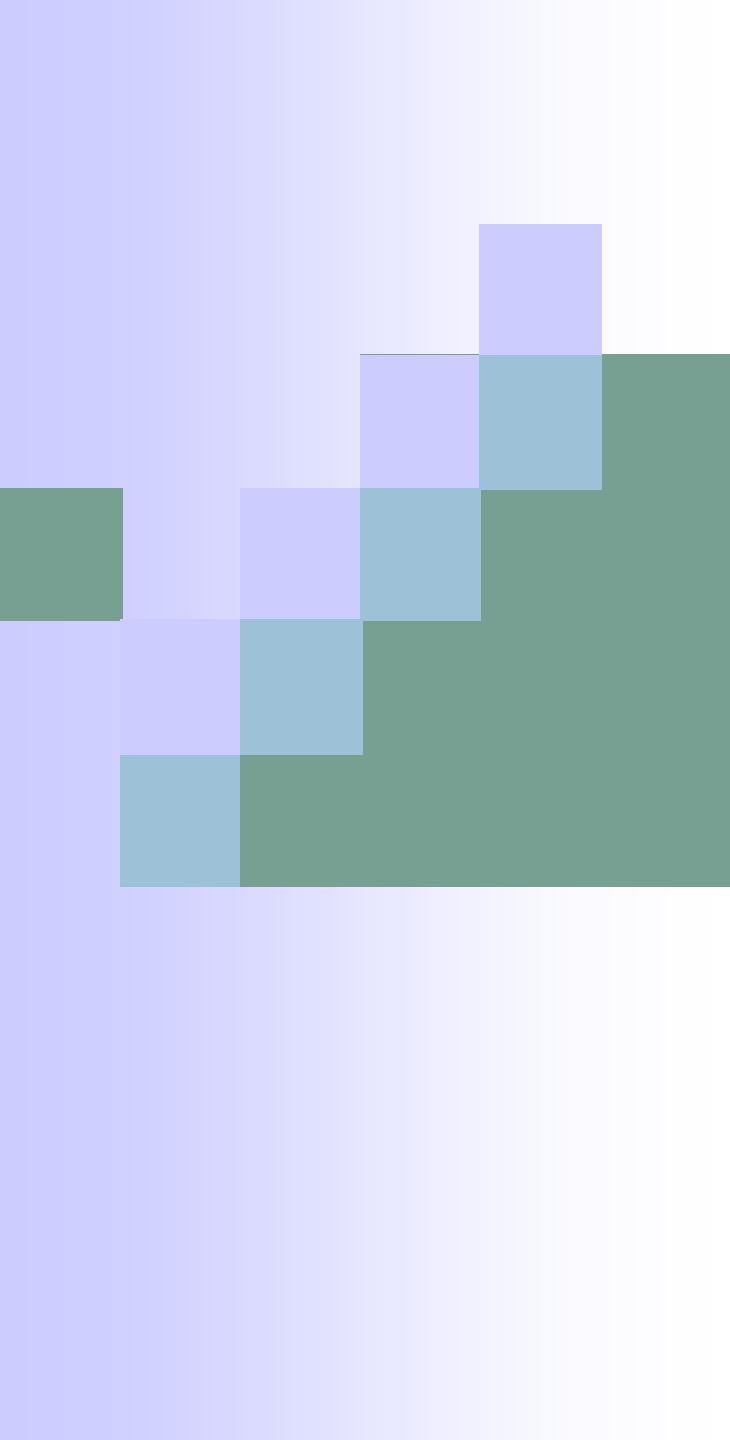
# Otros protocolos de la capa de red

## ➤ **IPX**

- En desuso, utilizado principalmente por redes implementadas con el Sistema Operativo Novell Netware
- No se asignan direcciones estáticas a los equipos, estos se autoconfiguran mediante broadcasts

## ➤ **NETBEUI**

- En desuso, utilizada por los Sistemas Operativos de Microsoft basados en MSDOS
- No utilizan identificadores numéricos sino nombres descriptivos que se propagan en la red por medio de broadcasts



# Capa 4

# Transporte

# Funciones

- Segmentación de datos de las capas superiores
- Establecimiento de operaciones de extremo a extremo
- Envío de los segmentos al destino
- Asegurar la fiabilidad de los datos
- Establecer un control de flujo

# Fiabilidad

- La capa de Enlace de datos también tenía esta función
- En capa implementación de la arquitectura de red se decidirá cual de ellas debe encargarse de la fiabilidad (o las dos, o ninguna)
- Se utilizan los mismos conceptos que en la capa de enlace de datos



# Control de Flujo

- Similar a la función existente en la capa de Enlace de datos pero dirigida a la capa de Transporte
- Uno de los sistemas más habituales se denomina **windowing**
  - Origen y destino se ponen de acuerdo en cuantos segmentos enviar de forma simultanea
  - Se envían uno tras otro sin esperar confirmación
  - El receptor mandará un acuse de recibo por cada uno de los recibidos
  - El emisor reenviará solo aquellos que no han sido recibidos correctamente

# Protocolos del modelo TCP/IP

## ➤ TCP

- Transmission Control Protocol
- Permite que la información transmitida se reciba sin errores
- Los segmentos se envían a destino y se reensamblan en el orden indicado por el emisor
- Si falta algún segmento se solicita su retransmisión antes de enviar los siguientes segmentos reensamblados a capas superiores

## ➤ UDP

- User Datagram Protocol
- No utiliza control de flujo. Este debe ser controlado por las aplicaciones de las capas superiores
- Los segmentos se envían a destino y se envían a las capas superiores tal y como son recibidos
- Si algún segmento se recibe fuera de orden, se desecha
- No se solicita la retransmisión de los segmentos que no llegan o lo hacen incorrectamente

## ➤ Puertos

- Tanto TCP como UDP crean un puerto para comunicarse con el otro extremo
- Ese puerto es identificado por medio de un número de 16 bits
- Los puertos se refieren a una zona de memoria en la que se almacenan los datos a transmitir o recibir
- Los puertos TCP por debajo de 256 se denominan **puertos bien conocidos** y se reservan para servicios estándar (de la capa de aplicación)

## ➤ Algunos puertos

Puerto/Protocolo	Descripción
20/tcp	<a href="#">FTP</a> File Transfer Protocol (Protocolo de Transferencia de Ficheros) - datos
21/tcp	<a href="#">FTP</a> File Transfer Protocol (Protocolo de Transferencia de Ficheros) - control
22/tcp	<a href="#">SSH</a> , <a href="#">scp</a> , <a href="#">SFTP</a>
23/tcp	<a href="#">Telnet</a> manejo remoto de equipo, inseguro
53/udp	<a href="#">DNS</a> Domain Name System (Sistema de Nombres de Dominio)
80/tcp	<a href="#">HTTP</a> HyperText Transfer Protocol (Protocolo de Transferencia de HiperTexto)
123/udp	<a href="#">NTP</a> Protocolo de sincronización de tiempo
137/tcp	<a href="#">NetBIOS</a>
443/tcp	<a href="#">HTTPS/SSL</a>
1433/tcp	Microsoft-SQL-Server
1521/tcp	<a href="#">Oracle</a> listener
3306/tcp	<a href="#">MySQL</a>
3389/tcp	RDP ( <a href="#">Remote Desktop Protocol</a> )
3690/tcp	<a href="#">Subversion</a>
5432/tcp	<a href="#">PostgreSQL</a>
8080/tcp	<a href="#">HTTP HTTP-ALT</a> Alternativa al puerto 80

## ➤ **Funcionamiento del Router: Redireccionamiento de Puertos**

- Esta asociado al NAT
- Permite redireccionar un puerto del router a un puerto de un equipo de la red interna
- De esta manera varios equipos de la red interna pueden dar servicio al exterior
- Para acceder desde el exterior al servicio, hay que conocer el puerto que se está utilizando en el router para redireccionar





# Capa 5

## Sesión

# Funciones

- Establecer, administrar y finalizar sesiones de comunicación entre las aplicaciones de emisor y receptor
- Control de diálogo
  - **Semiduplex**: Cuando una aplicación transmite, la otra debe esperar. Los datos no pueden cruzarse en la línea
  - **Full Duplex**: Las dos aplicaciones pueden transmitir cuando deseen. Los datos pueden cruzarse en la línea
- No existe en el modelo TCP/IP



# Capa 6

# Presentación

# Funciones

- Encargada de que el receptor pueda comprender los datos
- Funciones Principales:
  - Formateo de datos (p.e. conversión de ASCII a EBCDIC)
  - Compresión
  - Cifrado
- Estándares de la capa
  - Imágenes estáticas (JPEG, TIFF)
  - Imágenes en movimiento (MPEG, QuickTime)
  - Audio (MIDI)
- No existe en el modelo TCP/IP



# Capa 7 Aplicación

# Funciones

- Brinda servicios de red a las aplicaciones de los usuarios
- Las aplicaciones deberán encargarse de aquellas funciones que no están presentes en los protocolos de las capas inferiores (compresión, cifrado, ...)
- Protocolos
  - Asociados a la navegación web
    - http
    - https
  - Para transferencia de ficheros
    - ftp
    - tftp
  - De correo electrónico
    - pop / smtp
    - imap
  - Terminal remoto
    - telnet
    - ssh
    - rdp



# Nombres: fichero hosts

## ➤ Traducción de nombres

- Es más sencillo utilizar un nombre descriptivo que una dirección IP (especialmente con ipv6)
- Diferentes sistemas de traducción Nombre  $\leftarrow \rightarrow$  IP

## ➤ hosts

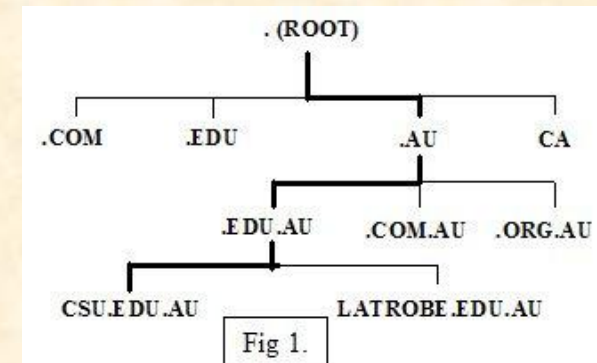
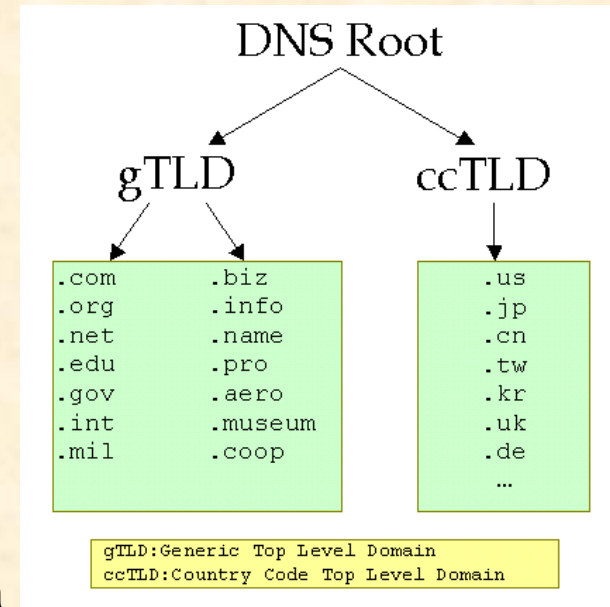
- Un fichero local mantiene una tabla de traducción.
- Cada equipo de la red tiene su propio fichero por lo que si hay alguna modificación, hay que hacerlo en todos.
- Nombre del fichero:
  - Windows: **%windir%\System32\drivers\etc\hosts**  
Normalmente %windows%=C:\Windows
  - Linux: **/etc/hosts**

# Nombres: NETBIOS

- Protocolo de Microsoft
- Puede instalarse en los linux (daemon nmbd)
- Es un protocolo de difusión
  - Los equipos se anuncian en la red.
- Los routers no propagan la difusión
  - Algunos routers pueden configurarse para ello pero la difusión del nombre no es posible si la infraestructura de la red pasa por routers fuera del control de la organización
- Si es necesaria la utilización del nombre NETBIOS en una red con routers hay que utilizar el servicio de nombres de Windows (WINS)

# Nombres: DNS

- Domain Name Services
- Organiza los nombres de los equipos en dominios en distintos niveles
  - TLD. Globales o específicos para cada país
  - 2LD. Asignados por la organización responsable del TLD para evitar duplicidades
- Las empresas u organizaciones se responsabilizan de su dominio pudiendo crear subdominios en otros niveles (3LD, 4LD...) libremente
- A partir de 2LD se pueden crear equipos
- Debe haber un servidor de nombres que se responsabilice de cada dominio (zona)
- Los servidores DNS se ponen en contacto entre si para que un cliente pueda conocer la dirección IP de equipos de cualquier zona
- Los nombres DNS de los equipos se generan de abajo a arriba en el árbol separando cada nombre por punto (".")
  - p.e. `www.google.com` indica un equipo llamado **www** en el 2LD **google** que está encuadrado en el TLD **com**



# DHCP

- Dynamic Host Configuration Protocol
- Se utiliza para configurar automáticamente los valores IP de los equipos (en lugar de utilizar configuración manual para cada equipo)
- Debe haber un equipo (servidor DHCP) encargado de repartir las direcciones
  - Las direcciones las repartirá en la red en la que tenga configurado el adaptador de red desde el que le llegan (ámbito)
  - Además de Dirección IP y máscara puede proporcionar otros valores como puerta de enlace o servidores de nombres
  - Si un equipo no encuentra un servidor se autoasigna una dirección dentro de la red 169.254.0.0/16
- Las solicitudes por parte de los clientes se realizan por broadcast
- Hay que tener cuidado si se tienen varios servidores DHCP para evitar que repartan la misma dirección a varios equipos diferentes
  - Si hay varios servidores el cliente solo aceptará el ofrecimiento de uno de ellos pero no se puede controlar de cual
- La dirección se da por un tiempo limitado por lo que los clientes deben solicitar su renovación periódicamente
- El servicio se puede configurar para que a un equipo se le asignen siempre los mismos valores IP

