unir
LA UNIVERSIDAD DE INTERNET

FORMACIÓN PROFESIONAL

UNIDAD FORMATIVA 4

Networking

Conceptos de networking

Índice

Conceptos de Networking

En el mundo actual, la ubicuidad de las redes de ordenadores hace que frecuentemente nos olvidemos de la complejidad que supone tener tantísimos sistemas interconectados, comunicando información de unos a otros a través de internet, redes móviles o incluso en las redes locales de cada hogar.

En esta sección revisaremos los fundamentos de las redes de ordenadores desde su concepción, detallando cómo se usa el medio físico para el intercambio de las unidades elementales que conforman el ADN de las redes: los bits.

Para que este estudio sea riguroso y completo, existen unos modelos de referencia que nos aportan una aproximación al problema de cómo enviar información de un lugar a otro empleando un modelo de *capas* o niveles. Estos niveles, relacionados entre sí usando *servicios* y *protocolos*, conforman el núcleo de lo que se estudiará en esta unidad: IP, TCP, HTTP… Estas siglas están tan presentes en el día a día del trabajo del técnico que ya no se les presta la debida atención.

Para terminar la sección, se revisarán los fundamentos del intercambio eléctrico de información entre dos entidades, usando para ello las capas correspondientes de los modelos de referencia estudiado, en los que la información viaja siempre en vertical: de este modo dejaremos abierta la puerta al siguiente tema, que tratará de protocolos de un nivel superior, pero que asumen que la información requerida puede ser transmitida, sin importar los medios físicos a través de los que lo hace.

Objetivos

- Comprender el concepto de red.
- Entender la diferencia entre los niveles de red en los modelos de referencia: OSI y TCP/IP.
- Conocer los fundamentos de la transmisión de paquetes a nivel físico y de enlace.

Definición de red

La definición que da el libro de referencia en redes de ordenadores, el famosísimo y recomendado *Tanenbaum*, es la siguiente (traducción libre del inglés):

"El modelo tradicional de un único ordenador para todas las necesidades de computación de una organización ha sido reemplazado por un modelo en el que un gran número de ordenadores independientes pero interconectados realizan el mismo trabajo. Estos sistemas se denominan ***redes de ordenadores."***

Se observa que esta definición no habla de *servidores y clientes* ni de centros de datos ni de proveedores de nube. De hecho, los autores usan para su definición la diferencia principal frente un ordenador monolítico: la interconexión de múltiples ordenadores.

Esto sigue siendo verdad a pesar de la cantidad de protocolos disponibles en el mercado. Por ejemplo, la tercera edición de *Tanenbaum* (de 1996) fue la primera en incluir referencias al protocolo 802.11, que ha definido y evolucionado el wifi que hay ahora disponible en cualquier bar. Los autores incluso han incorporado un apartado sobre RFID, el protocolo que hace funcionar las tarjetas de proximidad, en la última versión.

Criterios de clasificación

Las redes de ordenadores pueden clasificarse atendiendo a varios criterios. En función del problema a tratar se usará un criterio u otro.

Administración

Desde el punto de vista de un administrador, una red puede ser una red **privada**, que pertenece a un único sistema autónomo y no se puede acceder fuera de su ámbito físico o dominio lógico, o también puede ser **pública**, a la que todos pueden acceder.

En este sentido, una red casera formada por un dispositivo ADSL o de fibra y los equipos informáticos conectados a ella con o sin cable (ordenadores, teléfonos móviles, televisores, impresoras, etc.) es una red privada. La red pública por antonomasia es internet.

Interconectividad

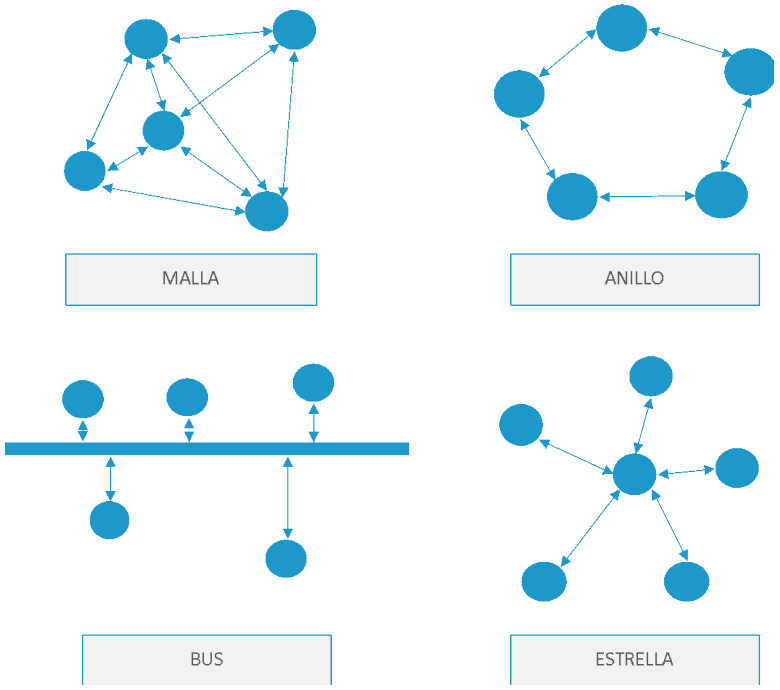
Los dispositivos pueden conectarse entre sí de diferentes maneras. Esta conectividad puede ser lógica, física o combinada y existir a diferentes niveles.

- En una red **mesh** cada dispositivo se puede conectar a cualquier otro dispositivo en la red, creando una malla. Una red peer-to-peer es un caso de red mesh a nivel de aplicación; una red wifi sin punto de acceso es una red mesh a nivel de acceso al medio.

- Una red de tipo **bus** conecta todos los dispositivos a un único medio. Una red local Ethernet cableada es un caso de bus a nivel físico.

- En una red en **anillo,** cada dispositivo está conectado a sus pares izquierdo y derecho únicamente, creando estructuras lineales.

- En una red en **estrella,** un dispositivo central tiene conexiones a cada uno de los demás dispositivos. Una red wifi con punto de acceso (el tipo habitual) es de tipo estrella: el tráfico entre dos ordenadores debe atravesar el router wifi.



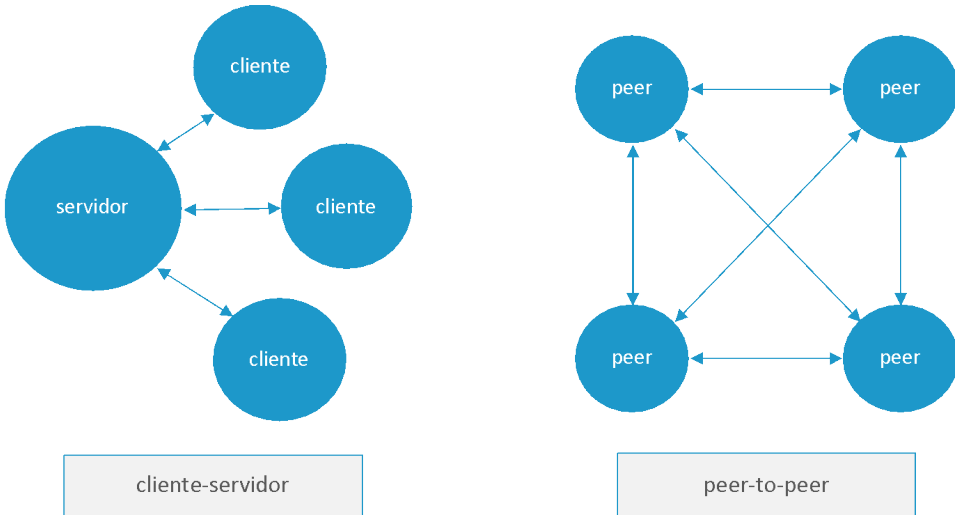
Tipos de redes según su esquema de conexión.

Arquitectura

Este criterio se refiere al rol que cumplen los dispositivos que pertenecen a la red:

- Puede haber uno o más sistemas que actúen como servidores. Un cliente solicita al servidor que atienda las solicitudes. El servidor toma y procesa la solicitud en nombre de los clientes.

- Dos sistemas pueden estar conectados punto a punto y formar una red peer-to-peer. Si ambos residen en el mismo nivel, se les denomina pares.



Tipos de redes según su arquitectura.

Extensión geográfica

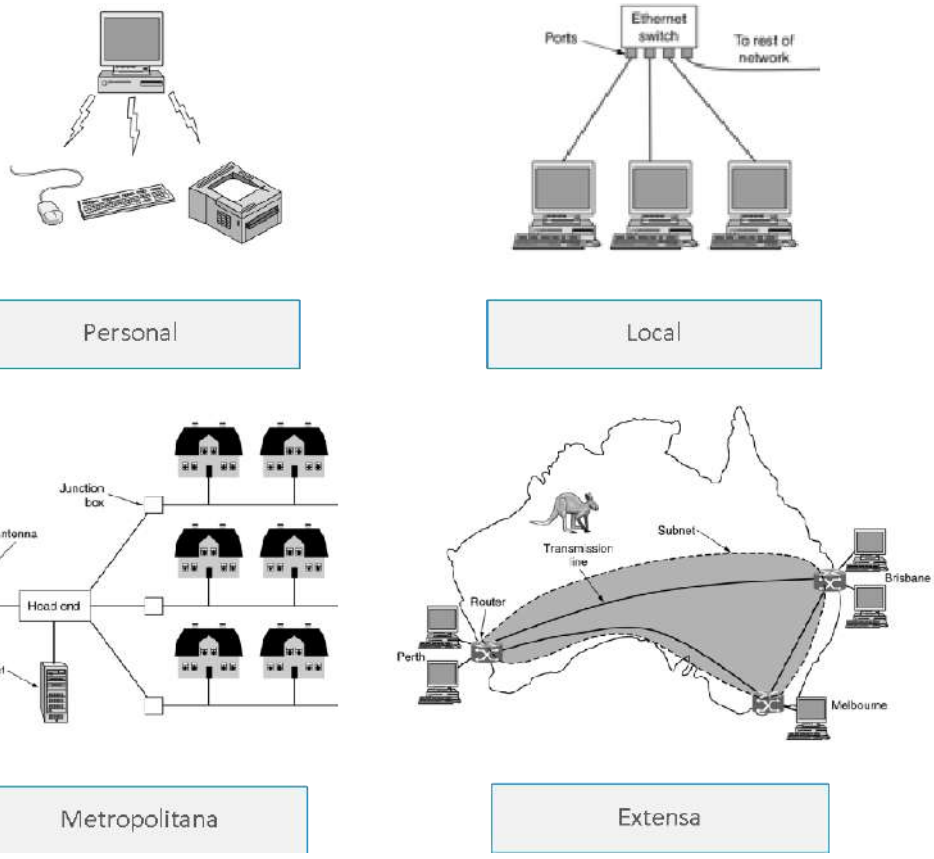
Atendiendo a la extensión geográfica, las redes se pueden clasificar en:

- **Redes de área personal (PAN):** aquellas con un alcance de hasta 10 metros. Pueden incluir dispositivos habilitados para bluetooth o dispositivos habilitados para infrarrojos.

- **Redes de área local (LAN):** aquellas que abarcan una oficina o un edificio y están operadas bajo un único sistema administrativo. Normalmente, una LAN abarca un hogar, una oficina o un edificio, pero puede abarcar una extensión de un campus de universidad. El número de sistemas conectados en LAN puede variar desde al menos dos hasta 16 millones. Es la tipología habitual para compartir los recursos como impresoras, servidores de archivos o incluso acceso a internet por parte de dispositivos de una misma ubicación.

- **Redes de área metropolitana (MAN):** aquellas que cubren una ciudad. Se pueden citar como ejemplos las redes de televisión por cable y las redes WiMAX, aunque solo han tenido aceptación en algunos países.

- **Redes de área amplia (WAN):** cubren una extensa zona geográfica que puede expandirse a través de provincias o países. Una WAN tiende a interconectar otras redes. Por ejemplo, cada sucursal de una organización puede tener una LAN para compartir el acceso a internet y las impresoras, mientras que una WAN mediante MPLS conecta todas las LANs para permitir el acceso a una aplicación corporativa ubicada en una oficina principal.



Tipos de redes según su extensión.

Se podría aquí añadir otro tipo de redes, conocidas como las **redes privadas virtuales** (VPN). Este tipo de redes se estudiarán más a fondo en la lección dedicada a seguridad en redes, pero tiene sentido estudiarlas en este contexto, pues permiten unir de forma segura dos extremos de una red (no importa la distancia que los separe) a través de un túnel por el que las conexiones van cifradas.

Modelos de redes

La transmisión de datos entre dos equipos, que es el objetivo final de la ingeniería de red, es una tarea que debe solucionar múltiples problemas físicos y lógicos a base de elementos hardware y software.

Para facilitar el diseño, implementación, solución de errores y, en general, el razonamiento sobre estos problemas, se modela el problema agrupando funcionalidades o responsabilidades comunes en múltiples niveles o **capas**. Cada capa resuelve una serie de problemas, liberando a las otras capas de estos problemas y limitando el flujo de intercambio de datos entre capas a las **inmediatamente contiguas.**

Los agentes implicados en los modelos son los ***hosts***: un *host* se puede referir a cualquier elemento de la red (un switch, un router, un amplificador de señal, una interfaz de red, etc). Básicamente, cualquier equipo que actúa en la red, es decir, que recibe y envía tráfico en cualquiera de las capas, puede ser considerado un host.

Arquitectura en capas

En la arquitectura en capas, todo el proceso de intercambio de tráfico de red se divide en pequeñas tareas. Cada tarea se asigna a una capa determinada que funciona de manera dedicada para procesar esa tarea específica. De esta forma, cada capa se encarga de todos los detalles de un trabajo concreto. Cada capa suele solucionar varios problemas a las capas superiores.

En el sistema de comunicación por capas, una capa de un host se ocupa de la tarea realizada por su capa homónima en el mismo nivel, en el host remoto. En el envío, la capa del nivel superior compone un paquete de datos y le delega el envío a la capa inmediatamente por debajo de ella. Esta segunda capa hará lo propio, añadiendo cabeceras que servirán para resolver los problemas de los que se encarga esta capa. Durante la recepción se sigue el camino inverso: los datos llegarán a la capa inferior, que desempaquetará los datos y los entregará a la capa inmediatamente por encima.

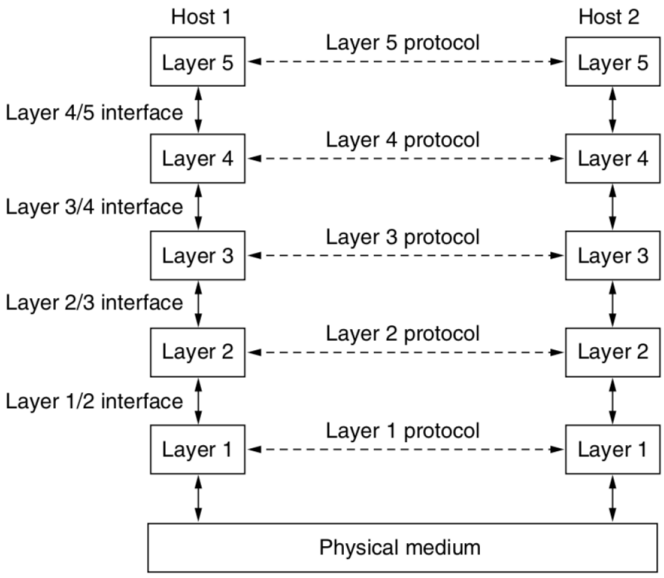


Imagen 1. Capas de red.

Todas las capas identifican a sus *peers* (contrapartes, la capa equivalente en el host del otro extremo) encapsulando el contenido en ***tramas*** *(frames)* con una cabecera que incluye los parámetros específicos de esa capa. El diagrama de la Imagen 2 muestra cómo cada capa añade una cabecera, de forma que los datos más la cabecera de la capa N se convierten en los datos de la capa N-1.

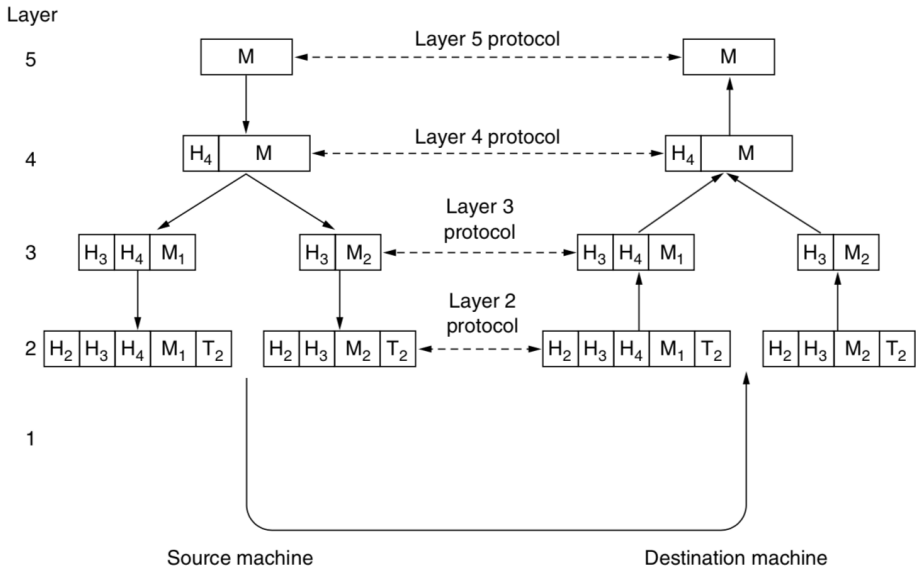


Imagen 2. Cabeceras añadidas en cada capa de red.

De manera formal, cada capa ofrece un ***servicio*** a la capa superior. Por ejemplo, la capa N puede ofrecer garantías de entregas sin errores a la capa N+1. Las reglas para el funcionamiento interno de una capa definen un ***protocolo***. Una capa ofrece un servicio mediante una *interfaz*, es decir, una serie de primitivas de software a modo de funciones con sus parámetros. Si se hace necesario cambiar la implementación de un protocolo (por ejemplo, para eliminar un bug) pero se mantiene la interfaz, solo será necesario modificar los componentes de una capa, de manera que se reduce la complejidad y el alcance del cambio.

¿Os suena? Esta es precisamente la abstracción que se usa en el diseño de clases en los lenguajes de programación orientados a objetos. La diferencia es que aquí hablamos de interfaces a nivel de red, no de una implementación en código fuente.

Modelos de referencia

Se estudian dos modelos de red principales: el modelo **OSI** y el modelo **TCP/IP**. El modelo OSI no ha llegado a ver una implementación en la industria y, por tanto, sus protocolos no se usan. No obstante, el diseño se usa extensivamente. El modelo TCP/IP, por el contrario, tiene como punto fuerte sus protocolos, ya que es el estándar *de facto* en las redes de ordenadores e internet.

Modelo OSI

La ISO, *International Organization for Standardization* (en español, Organización Internacional de Estandarización) publicó en 1980 el estándar OSI, de *Open Systems Interconnection*. OSI es un estándar abierto para cualquier sistema de comunicación formado por **siete capas** detalladas en la siguiente imagen:

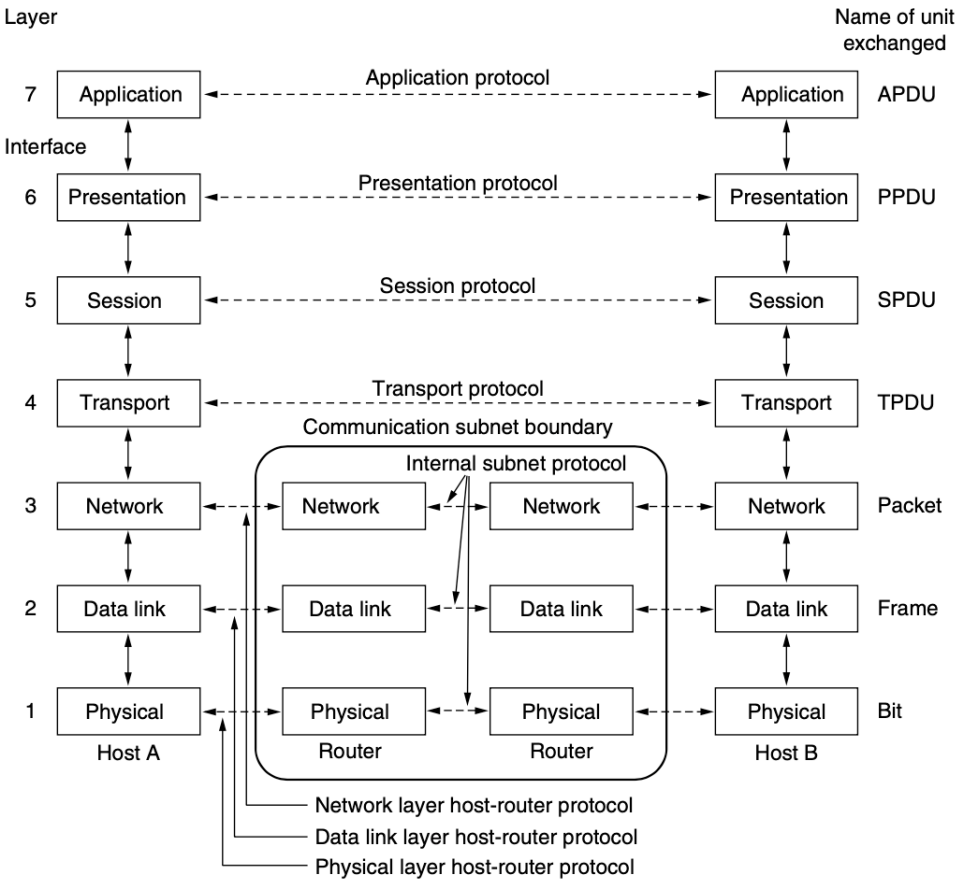


Imagen 3. Modelo de referencia OSI.

Aquí se ilustran las siete capas del modelo, con los servicios y protocolos marcados entre capas y niveles, y la nomenclatura de la unidad de datos intercambiada entre ellos. Vamos a ver con más detalle esos niveles:

Nivel físico

Define el hardware, cableado, potencia de salida, pulso, frecuencias, longitud de onda, ancho de banda.

Nivel de enlace de datos

Interactúa directamente con la capa física para convertir los datos en el elemento físico de la transmisión. También se encarga de detectar y corregir errores de transmisión.

Nivel de red

Es responsable de la asignación de direcciones de hosts en una red y el enrutamiento de paquetes.

Nivel de transporte

Es responsable de la entrega de extremo a extremo entre hosts, es decir, los nodos intermedios entre origen y destino no deberían afectar a este contenido. También se encarga de dividir los paquetes del tráfico de la aplicación en unidades más pequeñas y de asegurar la entrega en orden.

Nivel de sesión

Establece y mantiene un concepto de sesión durante la comunicación a partir de un establecimiento inicial, por ejemplo, a partir de una autenticación a base de credenciales.

Nivel de presentación

Define cómo traducir el contenido al formato nativo del host destino.

Nivel de aplicación

Es responsable de proporcionar interfaz al usuario de la aplicación. Incorpora las funcionalidades que interactúan con el usuario final.

Modelo TCP/IP

Internet utiliza la suite de protocolos TCP/IP, por lo que este modelo se puede denominar también **modelo de internet.** El modelo OSI es un modelo de comunicación general, pero el modelo TCP/IP es una colección de protocolos concreta utilizada en internet y en multitud de redes privadas. Mientras que el modelo OSI precedió a los protocolos OSI, la implementación de TCP/IP vino primero y el modelo se definió después.

Sin entrar en detalles sobre su historia, los criterios que dieron pie a TCP/IP fueron:

- Resistencia a la pérdida de elementos de red sin afectar al tráfico existente.
- Arquitectura flexible capaz de soportar tanto transferencia de ficheros como tráfico en tiempo real.
- Interconexión de redes heterogéneas: cableadas, radio, satélite…
- Posibilidad de mantener una conexión, incluso en el caso de caída de nodos intermedios, entre la fuente y el destino.

El modelo TCP/IP elimina o unifica varias de las capas del modelo OSI, eliminando complejidad a la hora de la implementación, pero sin perder funcionalidad. Las capas definidas en este modelo son:

Enlace

Este nivel no cuenta con mucha documentación incluso en el modelo original: su propósito principal está en definir qué deben hacer los enlaces, como conexiones Ethernet o conexiones serie, para poder usarse por la capa superior para establecer comunicaciones sin necesidad de una conexión permanente. Es poco más que el enlace entre el hardware y la capa que veremos ahora.

Internet

Esta capa, cuyo nombre ha dado nombre a la red que todos conocemos, es la encargada de llevar paquetes de una red a otra, en cualquier orden y a través de cualquier medio. Utiliza para esto el **protocolo IP** (*protocolo de internet)* y se apoya en un protocolo de control llamado ICMP (*Internet Control Message Protocol)*. Esta capa define el direccionamiento (cómo identificar a diferentes hosts en una red determinada), el enrutamiento (cómo llevar un paquete, salto a salto, hasta una red destino) y la gestión de errores a nivel de paquete.

Transporte

Esta capa se construye sobre el protocolo IP y ofrece dos protocolos principales:

- TCP es un protocolo de transporte orientado a conexión que garantiza que dos entidades puedan compartir streams de bytes, que llegan de forma ordenada y sin congestionar al destino.
- UDP (*User Datagram Protocol)* es otro protocolo de transporte, sin conexión y sin garantías de entrega, lo que se denomina un protocolo *best-effort*. Su ventaja frente a IP es la mayor velocidad al no tener la compleja capa de gestión de conexión, control de flujo y entrega ordenada de paquetes. La gran desventaja es, sin duda, que no se puede confiar que un paquete llegue al destino: esto es muy útil en transmisión de vídeo en tiempo real, donde lo importante es que los paquetes lleguen a tiempo (si llegan tarde, ya no son necesarios).

Aplicación

El nivel de aplicación de TCP/IP absorbe los anteriores niveles de sesión y presentación, y representa todos los protocolos que se construyen por encima de las capacidades de entrega de TCP y UDP, de los que veremos más adelante detalles: DNS, HTTP, FTP, SSH…

Introducción a la capa física

La capa física es la responsable de definir cómo trabaja el hardware de red, las propiedades de los cables, las frecuencias y modulaciones, etc. En el modelo OSI, es la única capa que hace referencia a la conectividad física entre dos equipos, ya que el resto de las capas trabajan con abstracciones de software. Esta capa **no está definida** en el modelo TCP/IP, por lo que se suele usar OSI para su definición y estudio.

Deterioro de la transmisión

Las señales tienden a deteriorarse cuando viajan a través del medio por diversas razones, por ejemplo:

- **Atenuación:** la potencia de la señal (o más concretamente, la densidad de potencia de la señal) se reduce a medida que esta se transmite por el medio. La señal debe tener suficiente potencia en la recepción para que el receptor pueda interpretarla correctamente.

- **Dispersión:** a medida que la señal viaja a través del medio, la banda de frecuencia tiende a extenderse y solaparse.

- **Retardo:** aunque el protocolo define la velocidad y frecuencia de transmisión, los equipos pueden tener defectos en el hardware que hagan que los parámetros varíen. Si la velocidad de la señal y la frecuencia no coinciden en ambos extremos, hay posibilidades de que la señal llegue al destino de manera arbitraria.

- **Ruido:** se llama ruido en la señal a la perturbación aleatoria que tiene la capacidad de distorsionar la información real que se está transmitiendo. Se pueden identificar, entre otros:

    - Ruido térmico: producido por la agitación de los conductores electrónicos del medio.

    - Intermodulación: producido en transmisiones en banda cuando la frecuencia usada por un canal no se limita adecuadamente y solapa con otros canales.

    - Crosstalk: producido por señales ajenas a la transmisión, pero que comparten el mismo medio.

    - Impulso: producido por perturbaciones irregulares e instantáneas.

Medios de transmisión

A grandes rasgos, los medios de transmisión se pueden clasificar en guiados y no guiados:

- **Medios guiados**: cualquier cable, ya sea de coaxial, de cobre o de fibra óptica, es un medio guiado. El cable puede conectar punto a punto dos dispositivos o conectar varios en una arquitectura de bus.

- **Medios no guiados**: son aquellos en los que no hay un material físico que dirija la señal a su destino. Cualquier dispositivo podría recibir la transmisión por el mero hecho de estar dentro del alcance de la transmisión.

Multiplexación

La multiplexación es la técnica que permite aprovechar un medio para enviar más de un flujo continuo de información. En la fuente, un sistema multiplexor combina los flujos o ***canales*** y los transmite en un único medio. En el destino, un *demultiplexor* extrae cada canal y lo entrega de manera individual.

Las tres técnicas principales de multiplexación son **por división de Frecuencia, de Tiempo** o **por Código.**

Estas técnicas se pueden combinar. Por ejemplo, la comunicación digital móvil de segunda generación, GSM, usa una combinación de FDMA y TDMA (la evolución a 3G cambió a CDMA).

Multiplexación por división de frecuencia (FDM)

Aprovecha la transmisión en bandas de frecuencia para compartir un canal. La transmisión de radio y televisión analógica sirve de ejemplo familiar: hay múltiples canales y cada canal ocupa un cierto ancho de banda (kHz en el caso de la radio, MHz en el caso de la TV).

El diagrama de la Imagen 4 muestra 3 canales en banda base (que podrían ser señales analógicas de telefonía de 4 KHz, por ejemplo) que son mezclados en 3 bandas diferentes. Cada canal mantiene su ancho de banda original, pero se transmite con una portadora, o frecuencia central, superior.

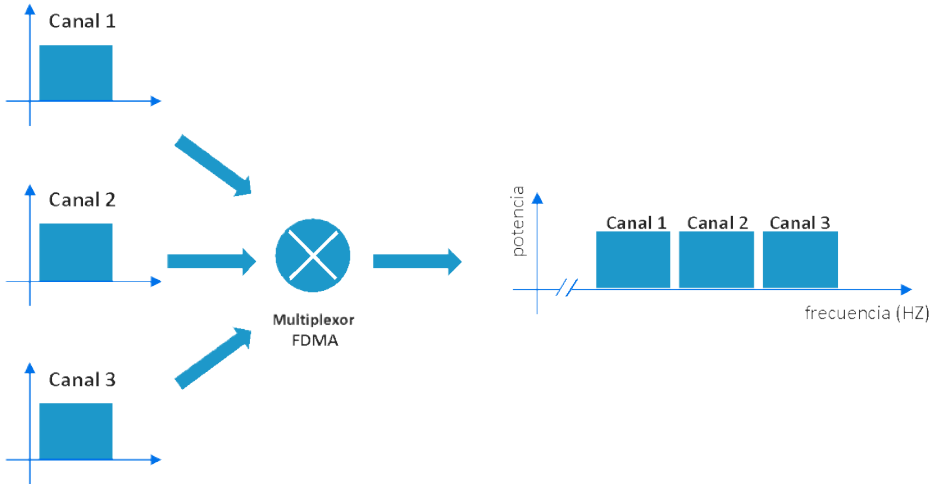


Imagen 4. Diagrama de FDMA. Elaboración propia.

Multiplexación por división de tiempo (TDM)

Divide el flujo de tiempo en un número fijo de intervalos. Por ejemplo, en una división en 3 intervalos se pueden multiplexar 3 canales, tal y como muestra la Imagen 5. Cada canal aprovecha todo el ancho de banda posible en su intervalo asignado. En esta técnica, el medio multiplexado debe usar una velocidad de transmisión más alta que la suma de velocidades de todos los canales.

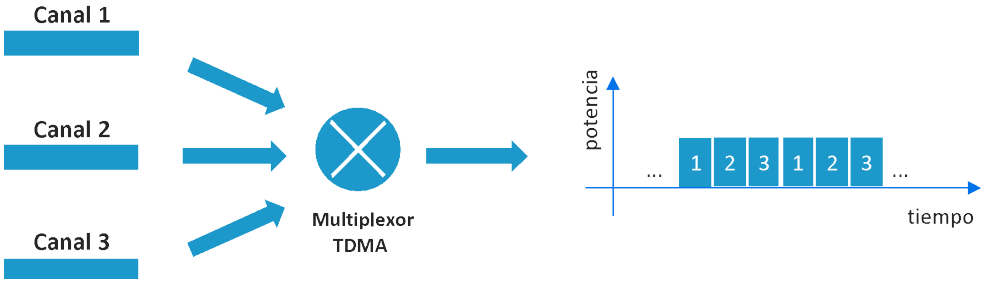


Imagen 5. Diagrama de TDMA. Elaboración propia.

Multiplexación por división de código (CDMA)

Convierte una señal de banda estrecha (el equivalente a un canal de FDMA, por ejemplo) en una señal de banda ancha mediante la **recodificación** de la misma. La multiplexación se consigue usando códigos diferentes para cada canal, codificados de forma que señales pertenecientes a diferentes emisores nunca se puedan confundir entre sí. La generación de este tipo de codificadores está fuera del ámbito de la asignatura, pero se puede averiguar más investigando sobre las funciones de Walsh.

Conmutación

La conmutación es el mecanismo que permite transmitir datos desde una fuente a destinos que no están conectados directamente. Los nodos de interconexión de la red reciben datos de fuentes conectadas directamente, los almacenan, analizan y finalmente los envían hacia el siguiente dispositivo de interconexión más próximo al destino.

A nivel general, la conmutación puede dividirse en dos categorías principales:

- **Sin conexión:** no se requiere ningún enlace previo y la confirmación de recepción es opcional.
- **Orientado a la conexión**: es necesario establecer el circuito a lo largo de la ruta entre ambos extremos antes de poder intercambiar tráfico. Los datos se envían entonces a lo largo del circuito. El circuito puede cerrarse nada más terminar la transferencia o puede mantenerse temporalmente para un uso posterior.

Conmutación de circuitos

En un sistema de conmutación de circuitos, los datos se transmiten a través de un **canal exclusivo**. Es necesario que estén especificados los datos que viajan por esa ruta, ya que no se permiten otros datos en la misma ruta. Además, el circuito debe estar establecido para que la transferencia de datos pueda tener lugar. Los circuitos pueden establecerse antes de la primera comunicación y mantenerse indefinidamente o establecerse y cerrarse a demanda para cada transmisión.

El ejemplo más claro de conmutación de circuitos es la telefonía analógica tradicional, ya que la señal viaja por un canal exclusivo, no compartido, durante toda la duración de la comunicación.

Conmutación de mensajes

La conmutación de mensajes está a medio camino entre la de circuitos y la de paquetes: cada mensaje se trata como una unidad y se transmite a lo largo de un canal exclusivo. Un conmutador de mensajes recibe el mensaje entero y almacena los datos temporalmente hasta que haya recursos disponibles para transferirlo al siguiente salto del circuito. El conmutador almacenará los datos y se mantendrá a la espera hasta que el conmutador del siguiente salto tenga suficientes recursos.

Al igual que en la conmutación de circuitos, la red debe reservar una **ruta exclusiva para la transmisión**. La conmutación de mensajes tiene dos inconvenientes principales:

- Cada dispositivo en la trayectoria del tránsito necesita capacidad de almacenaje suficiente para gestionar el mensaje entero.

- La técnica de almacenamiento y reenvío junto a la latencia debido a las esperas intermedias hacen que esta técnica sea muy lenta en comparación a la conmutación de paquetes.

La conmutación de mensajes se sustituyó por conmutación de paquetes al no ser una buena solución para los medios de transmisión en tiempo real.

Conmutación de paquetes

En la conmutación de paquetes, cada mensaje se fragmenta en paquetes de menor tamaño. El paquete lleva asociado una serie de cabeceras con información sobre el destino, control de errores, etc. Cada paquete con sus cabeceras se transmite de manera independiente al resto de paquetes.

La ventaja de la conmutación de paquetes respecto a la conmutación de circuitos es que se puede aprovechar mejor la capacidad de las líneas: un circuito reservado no permite la transmisión de más datos, incluso aunque en un momento dado ni emisor ni receptor estén enviando datos activamente. Los paquetes, sin embargo, pueden multiplexarse a la velocidad que permita la línea, por lo que los silencios de transmisión de un nodo pueden aprovecharse por otros.

Las redes IP son esencialmente redes de conmutación de paquetes, aunque dan soporte para calidad de servicio (QoS, Quality of Service), dando más prioridad a unos paquetes frente a otros.

Introducción a la capa de enlace

La capa de enlace de datos usa la interfaz de la capa física para pasarle tramas que esta convierte en pulsos eléctricos en un cable de cobre, en señales electromagnéticas en un protocolo inalámbrico, y en pulsos de luz en un cable de fibra óptica.

La capa de enlace de datos abstrae los conceptos físicos y la implementación hardware a las capas superiores. Actúa entre dos nodos que están conectados directamente en un mismo medio. Cuando en el mismo medio hay múltiples nodos, esta capa se encarga de evitar colisiones.

Es, por tanto, la capa encargada de **traducir los datos en parámetros** que el hardware puede convertir en señales físicas. El receptor recoge los datos del hardware, que están en forma de señales eléctricas u ópticas, los ensambla en un formato de reconocible y los entrega a la capa superior.

Las principales características de esta capa son:

- **Encapsulado**: la capa de enlace de datos toma los paquetes de la capa de red y los encapsula en tramas o *frames* que, luego, envía bit a bit al hardware. La capa de enlace del extremo receptor recoge las señales de hardware y ensambla las tramas en los paquetes que entrega a la capa de red.

- **Direccionamiento**: la capa de enlace de datos proporciona el mecanismo de direccionamiento de hardware. En esta capa, cada dirección es **única a nivel de enlace** y se codifica en HW durante la fabricación (en entornos virtuales, las direcciones pueden no ser globalmente únicas, pero los orquestadores son capaces de prevenir estas situaciones). Las direcciones MAC (*Medium Access Control*), se encuentran en las tarjetas Ethernet y wifi y permiten identificar unívocamente cada interfaz en un medio. Al contrario que las direcciones IP, las direcciones MAC no se usan para enrutamiento y son fijas (los switches Ethernet pueden usarlas para reducir el número de puertos por los que replicar un paquete, pero el concepto es diferente al de enrutamiento IP).

- **Sincronización**: los equipos involucrados en una transferencia deben sincronizarse antes de la misma, tanto para que usen la misma velocidad de bit como para detectar el principio de una trama.

- **Control de errore**s: las señales pueden encontrar problemas en la transmisión y los bits pueden estar invertidos. Como se verá más adelante, algunos errores se pueden detectar y notificar, mientras que otros se pueden corregir en destino.

- **Control de flujo**: los nodos en el mismo enlace pueden funcionar a diferentes velocidades. La capa de enlace de datos controla estas situaciones para que ambos nodos puedan trabajar a una velocidad común.

- **Acceso múltiple**: en medios compartidos es posible que dos nodos intenten emitir señales a la vez. Estas señales colisionan y se vuelven ilegibles por el receptor. La capa de enlace de datos es capaz de hacer uso de técnicas de multiplexación del acceso al medio como FDMA, TDMA o CDMA (ofrecidas por la capa física) para dar la capacidad de compartir el acceso entre múltiples sistemas o agentes.

Detección y corrección de errores

Los diferentes tipos de ruido mencionados anteriormente pueden provocar errores en la transmisión, volviendo los datos ilegibles. Las capas superiores trabajan sobre una vista generalizada de arquitectura de red y asumen, gracias al servicio ofrecido por la capa de enlace, que estos problemas no existen. La mayoría de las aplicaciones no funcionarán de forma esperada si reciben datos erróneos (las aplicaciones de voz y vídeo suelen ser tolerantes a fallos y pueden verse menos afectadas).

Detección de errores

Entre las técnicas de detección se pueden contar la comprobación de paridad, el uso de checksums y los algoritmos CRC. Todas estas técnicas implican enviar bits adicionales calculados a partir de los datos. En la recepción se vuelven a calcular estos bits a partir del mensaje y se comprueba que los bits calculados y los recibidos coincidan. Si los bits no coinciden, se considera que ha existido un fallo en la transmisión.

Comprobación de paridad

Se envía un bit adicional, típicamente por cada 8 bits de datos, de forma que el número de bits a 1 en total sea par. Si el número de bits de datos a 1 es par, se añade un bit de paridad en cada trama con el valor 0; si el número es impar, el bit de paridad tiene el valor 1, de manera que siempre hay un número par de unos.

El receptor solo necesita contar el número de unos en una trama. La trama se considera válida si el recuento de unos es par, incluido el bit de paridad. En caso contrario, la trama se considera dañada.

Esta técnica funciona si solo **se alterna un bit de la trama**. Si el número de bits erróneos es mayor, la comprobación de paridad puede dar falsos positivos.

Checksum

Los bits de paridad son un caso particular del concepto de checksum. Cualquier grupo de bits calculados a partir de los datos se puede considerar un ***checksum*** una vez añadidos a la cabecera de una trama. Por ejemplo, el checksum usado en las cabeceras IP se calcula como la suma de los bits del mensaje, una vez dividido en palabras de 16 bits. Este checksum es capaz de detectar errores indetectables por un bit de paridad. No obstante, es vulnerable a errores más típicos de hardware de mala calidad que debidos al ruido de la línea, como la inserción de ceros o la reordenación de palabras.

Comprobación de redundancia cíclica (CRC)

En esta técnica se transmite un código polinomial. Los bits de una trama de longitud N se consideran coeficientes de un polinomio de grado N-1. El código polinomial se calcula de manera que la trama y el código son divisibles por un polinomio que emisor y receptor han acordado antes de la transmisión. Si el cálculo de la división en el receptor tiene un resto diferente de cero, se puede asumir que algún bit ha cambiado de signo y la trama se ha corrompido en tránsito.

Corrección de errores

Hay dos modelos de corrección de errores:

- **Corrección de errores hacia atrás:** más que corregir, este modelo solicita la retransmisión de una trama cuando el receptor detecta un error. Este es el caso comentado en la sección anterior: se usa una técnica de detección para solicitar una retransmisión.

- **Corrección de errores hacia adelante:** cuando el receptor detecta algún error en los datos recibidos, ejecuta una técnica de autorrecuperación para corregir el error.

Hay **cuatro algoritmos de corrección de errores principales**: hamming, códigos binarios convolucionales, Reed-Solomon y códigos de validación de paridad de baja densidad. El detalle de estos algoritmos supera el alcance de esta asignatura. Basta decir que, por regla general, necesitan más bits de redundancia que un algoritmo de detección de errores.

Control de flujo

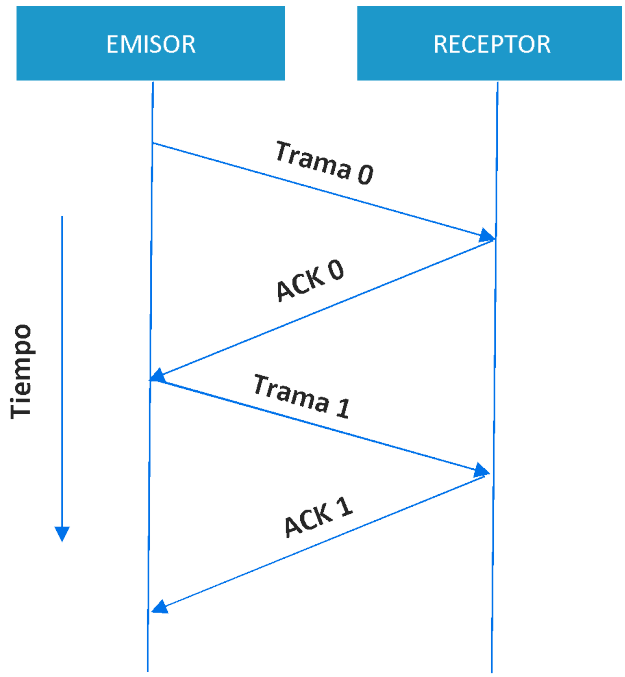
Cuando una trama se envía de un host a otro a través de un único medio, es necesario que el remitente y el receptor vayan a la misma velocidad. El control de flujo se encarga de asegurar que el emisor no envía datos (es decir, no activa señales eléctricas en el medio) más rápido de lo que el receptor va a poder actuar sobre ellos. Este problema es diferente al de la **sincronización**: el control de flujo asume que emisor y receptor transmiten a la misma velocidad (por ejemplo, 9600 bits por segundo), pero que el receptor puede estar haciendo otras tareas que le impidan aceptar una trama en un momento dado.

Para entender la situación se propone un escenario con un router conectado a 3 equipos. Las 3 conexiones son de 10 Mbps. Los nodos A y B envían tráfico al nodo C y empiezan a transmitir tramas a 10 Mbps. El router puede recibir tramas de A y B en paralelo, pero solo puede enviar uno de los flujos a C. El router podría almacenar las tramas en un buffer interno pero, dado que el buffer no va a ser infinito, la solución es controlar el flujo al que A y B envían las tramas. Cada trama se enviará a la velocidad de la línea, 10 Mbps, pero habrá tiempos de espera entre trama y trama que reducirán la velocidad efectiva a, idealmente, 5 Mbps para cada flujo.

Los siguientes apartados explican dos mecanismos de control de flujo: detención y espera (**stop and wait**) y ventana deslizante (**sliding window**).

Stop and wait

Cuando un emisor usa este mecanismo, se detendrá después del envío de una trama. Solo enviará la siguiente una vez haya recibido un acuse de recibo (ACK - *Acknowledge)* por parte del receptor. El cronograma de la imagen muestra un ejemplo sencillo en el que el emisor solo puede enviar una trama al recibir el ACK de la trama anterior.

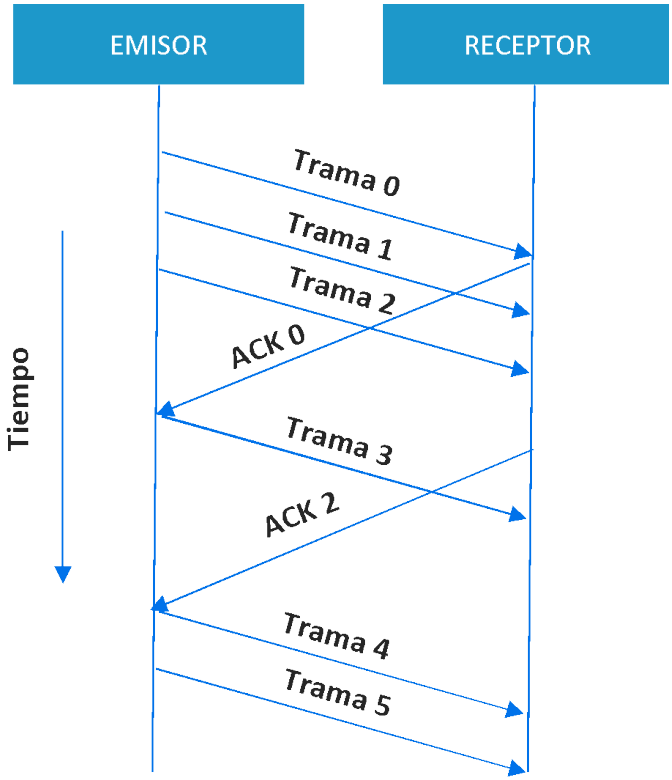


Esquema de control de flujo con stop and wait.

Ventana deslizante

En este mecanismo de control de flujo, el emisor mantiene un contador de tramas sin ACK. Tras enviar una trama, el emisor reduce el contador en uno. Cuando recibe un ACK, aumenta el contador en uno. Mientras el contador sea mayor que cero, el emisor es libre de enviar más tramas. Este protocolo aprovecha mejor el uso del canal que la técnica de stop and wait.

El cronograma de la Imagen 7 muestra un flujo con ventana deslizante de 3 tramas. Se puede observar que el receptor envía el ACK de la primera trama nada más recibirla. El emisor, al ver que hay un hueco libre en la ventana, puede enviar otra trama, pero solo una. El emisor retrasa el ACK de las tramas 2 y 3 hasta más tarde (por ejemplo, porque no ha podido procesarlas debido a una falta de recursos de CPU). En este caso puede enviar un único ACK para las dos tramas. A la recepción de este ACK el emisor puede enviar dos tramas más.



Esquema de control de flujo con ventana deslizante.

Referencias bibliográficas

El *Tanenbaum*, como es conocido en múltiples facultades, es la biblia de las redes de ordenadores. Su introducción pone al lector en contexto con el concepto de red con ejemplos de la vida diaria.

- *Tanenbaum, Andrew S. and Wetherall, David J. Computer Networks. Fifth Edition, Pearson New International ed. Boston [etc]: Pearson, 2014. Capítulo 1, introducción y apartado 1.1.*

LA UNIVERSIDAD EN INTERNET | FORMACIÓN PROFESIONAL

PROEDUCA