Teoría de Redes

Jose Antonio Lorencio Abril

1 Introducción a las redes de ordenadores

1.1 La red Internet

1.1.1 Componentes de Internet

Internet está conformado por millones de dispositivos, conocidos como hosts o sistemas finales, que ejecutan aplicaciones de red distribuidas. Estos dispositivos están conectados mediante enlaces de comunicación (cobre, fibra, radio), cada uno con un ancho de banda determinado.

También forman parte de esta red los equipos de interconexión, como son los routers y los conmutadores, cuya misión es el almacenamiento, procesamiento y reenvío de paquetes.

1.1.2 Hosts o Sistemas Finales

Los hosts o sistemas finales ejecutan aplicaciones de red distribuidas, se encuentran en el extremo de la red, los hay de diferentes tipos (ordenadores, smartphones,...).

Hay dos modelos de aplicaciones de red, que son el modelo cliente/servidor y el Peer-to-Peer (P2P).

1.1.3 Arquitectura de una aplicación cliente/servidor

El **servidor** procesa peticiones de los clientes. El host siempre está online, su dirección IP es estática y es común el uso de granjas de servidores.

Los **clientes** se comunican con el servidor pero no directamente entre sí, están conectados intermitentemente y sus direcciones IP son dinámicas.

1.1.4 Arquitectura de una aplicación P2P

No hay un servidor siempre online, sino una red de peers, que se comunican directamente entre sí,están intermitente conectados y tiene direcciones IP dinámicas. Es inherentemente escalable, aunque su gestión es compleja.

1.1.5 Tipos de redes de acceso

Las redes pueden ser de acceso residencial, institucional o móvil.

Se diferencian unas de otras por el ancho de banda, la calidad de servicio (ancho de banda garantizado, latencia máxima acotada o servicio de seguridad) y el hecho de ser una red dedicada o una compartida.

Redes de acceso residencial

- **ADSL (Assymetrix Digital Subscriber Line):** utiliza la red telefónica convencional pero con posibilidad de combinar datos y voz simultáneamente. Restringe la longitud de enlace. Soporta hasta 3.3 Mbps en el canal ascendente y 24 Mbps en el descendente.
- **HFC (Hybric Fiber Coaxial):** la red de cable y fibra una el hogar con el router del ISP (Internet Service Provider). Soporta hasta 216 Mbps en el canal ascendente y 1600 Mbps en el descendente. A diferencia del ADSL, el enlace hasta el router es compartido y su longitud no es un factor determinante. El despliegue lo hacen las compañías.
- **WiMAX (Worldwide Interoperability for Microwave Access):** utiliza ondas de radio para la transmisión. Alcanza hasta 70 Mbps en teoría, pero en realidad unos 20 Mbps.

Redes de acceso institucional

Son redes privadas pertenecientes a una empresa u organismo, también conocidas como intranet.

La configuración habitual consta de un router que da salida a la red Internet, hosts conectados entre sí mediante conmutadores que usan la tecnología Ethernet, y se utilizan puntos de acceso apra dar cobertura inalámbrica.

1.1.6 Medios de transmisión

- **Par trenzado:** pares de hilos de cobre dispuestos de forma helicoidal cubiertos por un aislante de plástico. Ampliamente utilizado en redes basadas en la tecnología Ethernet.
- **Cable coaxial:** núcleo de cobre recubierto por aislante envuelto en un conductor externo. Medio de transmisión originalmente empleado por las redes Ethernet y por las redes de TV por cable. Mayor coste, velocidad de transmisión e inmunidad al ruido que el par trenzado.
- **Fibra óptica:** la presencia/ausencia de luz codifica un bit. Se compone de un núcleo de fibra de vidrio de alta densidad, revestido con cristal o plástico de baja densidad. Es más costoso, más rápido y con mayor inmunidad al ruido, y con menor atenuación que el par trenzado y el cable coaxial. Es la opción preferida para los enlaces más largos.
- Otros medios no cableados, como microondas.

1.1.7 Interconexión de routers

Existen miles de redes interconectadas. Los mensajes se dividen en paquetes, que son almacenados, procesados y reenviados por los routers. Normalmente un paquete atraviesa varias redes hasta alcanzar su destino.

Hay dos formas de transportar los paquetes:

- **Conmutación de paquetes**: cada paquete se encamina en cada router de manera independiente, la entrega de los paquetes puede ser fuera de orden y no ofrece garantía alguna de calidad de servicio.
- **Conmutación de circuitos virtuales**: se establece una ruta fija para cada circuito que siguen todos los paquetes. La entrega de los paquetes se realizan en orden y con calidad de servicio garantizada.

Ambas modalidades requieren algoritmos de encaminamiento.

1.2 Conceptos básicos

1.2.1 Modos de comunicación

- **Símplex:** unidireccional.
- **Semi-dúplex:** bidireccional no simultánea.
- **Full-dúplex:** bidireccional simultánea.

1.2.2 Configuración del enlace

- **Punto a punto:** canal de comunicación individual entre pares de hosts.
- **Multipunto o difusión:** canal de comunicación compartido. Requiere de asignación del canal, estática o dinámica, y de arbitraje, centralizado o distribuido. Presenta diversas formas o topologías, como la malla, la estrella, la bus, o la anillo.

1.2.3 Escala de red

- **Redes de área local (LAN):** son redes privadas que abarcan pocos km. Configuradas como difusión (10/100/1000 Mbps), con una topología en anillo, bus o estrella, aunque su pequeño tamaño permite usar diseños específicos.
- **Redes de área extensa (WAN):** son redes públicas y/o comerciales, que abarcan muchos km. Configuradas como punto a punto (>1Gbps). El encaminamiento y la congestión son problemas a tener en cuenta, además, la topología es irregular.

1.3 Arquitectura de red

1.3.1 Necesidad de protocolos

Los protocolos de comunicación garantizan la interoperabilidad de los interlocutores. Un protocolo define el formato y el orden de los mensajes que se intercambian, y als aciones realizadas al enviar/recibir cada mensaje.

Protocolo: tanto los hosts como los equipos de interconexión siguen protocolos. Un protocolo debe tener una esècificación que defina sin ambigüedad los tipos de mensajes intercambiados, la sintaxis y semántica de los mensajes, y las reglas para determinar qué hacer, cuándo y cómo cada vez que se envía o recibe un tipo de mensaje concreto.

Los protocolos pueden ser de dominio público, definidos en RFCs (Request For Comments), o de propietarios, en cuyo caso su especificación no es conocida.

1.3.2 Necesidad de arquitecturas de red

Las redes son muy complejas, ya que tiene muchos componentes distintos, por lo que resulta consejable estructurar las redes en capas, ya que una estructura explícita permite identificar los componentes y sus relaciones en sistemas complejos, la modularización facilita el mantenimiento y la actualización, y los cambios en implementación de un servicio en una capa son transparentes para el resto del sistema.

Principios de la división en capas: una capa realiza un conjunto de tareas relacionadas. Además, cada capa proporciona servicios a al capa superior, usando únicamente servicios de la capa inferior a través de una interfaz.

Las entidades en la misma capa pero en diferenteshosts reciben el nombre de procesos pares, que dialogan entre sí mediante un protocolo.

El conjunto de capas y protocolos usados en cada capa se denomina arquitectura de red.

1.3.3 Arquitectura de capas de internet

Arquitectura TCP/IP: Tiene diversos niveles, de menor a mayor profundidad:

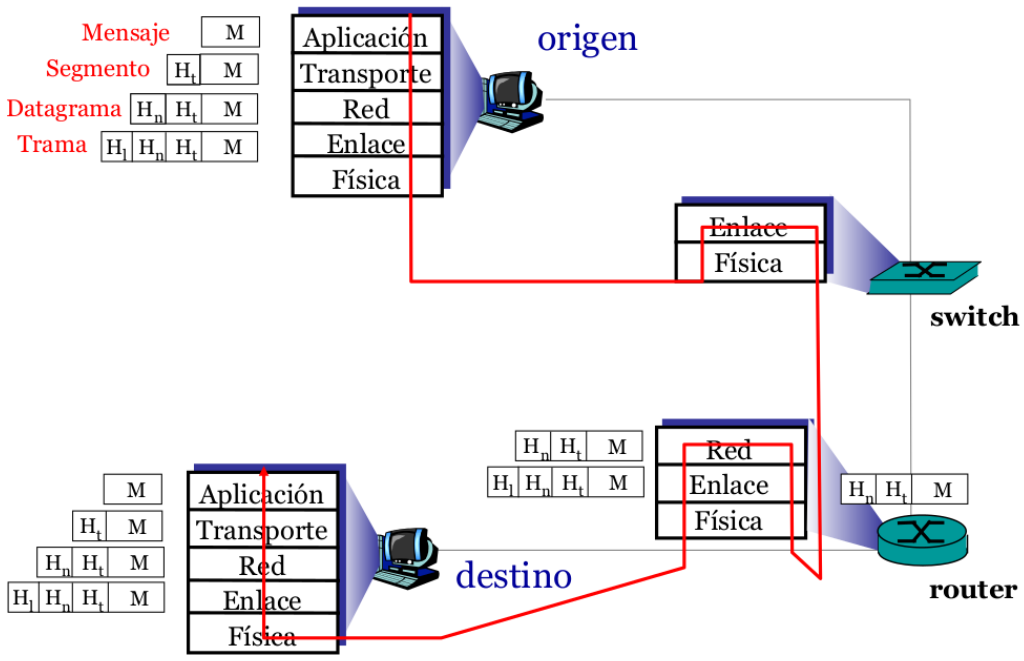
- **Aplicación**
- **Transporte:** se encarga de la transferencia de segmentos entre procesos, del control del flujo y la recuperación de errores, así como del control de la congestión. Protocolos TCP (Transmission Control Protocol) y UDP (User Datagram Protocol).
- **Red:** encaminamiento de paquetes entre el host origen y el host destino mediante algoritmos de encaminamiento. Protocolos IP (Internet Protocol), RIP (Routing Information Protocol), OSPF (Open Shortest Path First) y BGP (Border Gateway Protocol).
- **Enlace:** envía de tramas entre hosts y routers conectados directamente, hay detección de errores. Protcolo Ethernet, WiFi, PPP.
- **Física:** transmisión de un flujo de bits entre hosts y routers conectados directamente sobre un enlace físico.

Arquitectura de capas de ISO/OSI (Open System Interconnection) El modelo OSI incluye dos niveles adicionales entre aplicación y transporte.

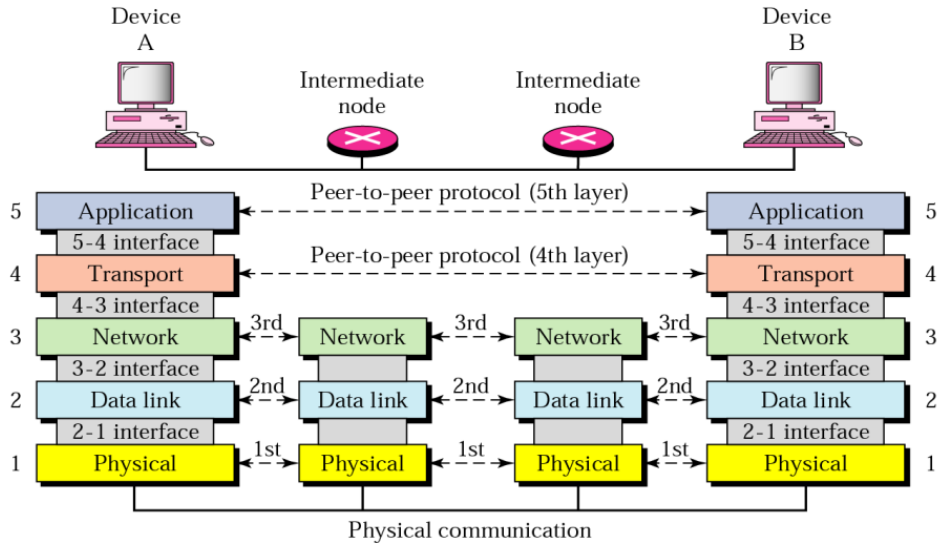
- **Presentación:** interpretación y tratamiento de los datos, cifrado, compresión y codificación.
- **Sesión:** sincronización y recuperación de los datos.

En la pila TCP/IP estas funciones corresponden al nivel de aplicación.

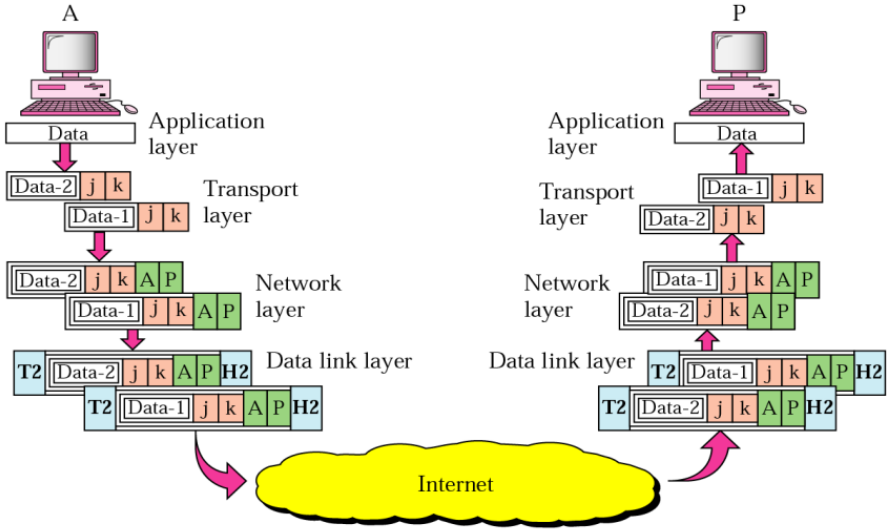
1.3.4 Encapsulación e independencia entre capas



1.3.5 Comunicación horizontal entre capas



1.3.6 Comunicación vertical entre capas



1.3.7 ATM

ATM (Asynchronous Transfer Mode) es una arquitectura basada en la conmutación de circuitos virtuales. Proporciona un servicio orientado a conexión, utiliza celdas de tamaño fijo de 53 bytes (5 de encabezado y 48 de datos), cada conexión es un flujo de celdas y maneja todo tipo de tráfico (servicio de transporte de tráfico en tiempo real y de no tiempo real). Además, gestiona la calidad del servicio.

Su arquitectura es extendida a 3 dimensiones:

- **Capas:** AAL (Application Adaption Layer) permite a otros protocolos utilizar ATM, ATM gestiona conexiones y celdas, y la capa física.
- **Los planos**, de usuario o de control.

- **La gestión de los planos.**

2 El nivel de transporte

2.1 Introducción

El objetivo del nivel de transporte es proporcionar un servicio de comunicación lógica entre procesos en hosts distintos a través de la red.

Este nivel involucra solo a los hosts **emisor**, que fragmenta los mensajes de las aplicaciones en segmentos y se los pasa al nivel de red, y **receptor**, que reensambla los segmentos de los mensajes y se los entrega a la aplicaciones.

Las funciones del nivel de transporte son:

- Comunicación de extremo a extremo: servicio de comunicación lógica entre procesos que se ejecutan en hosts distintos.
- Multiplexión y demultiplexión: identificar los procesos emisor y receptor sin ambigüedad.
- Detección de errores: identificar y descartar segmentos erróneos.
- Segmentación y reensamblaje: fragmentar y reensamblar la información del nivel de aplicación para ajustarse al tamaño máximo de trama del nivel de enlace.
- Control de flujo: regular el tráfico para evitar que un emisor rápido inunde a un receptor lento.
- Recuperación de errores: resovler situaciones anómalas.
- Control de la congestión: evitar que se saturen enlaces o equipos de interconexión.

Los protocolos utilizan el servicio de encaminamiento de paquetes entre hosts proporcionados por el nivel de red. Los **protocolos de transporte disponibles en internet** son **TCP** (Transmission Control Protocol), con entrega garantizada y en orden de los segmentos, control de flujo y de la congestión y recuperación de errores, y **UDP** (User Datagram Protocol), con entrega no garantizada y desordenada de los segmentos.

Ninguno de ellos ofrece garantías de latencia o de ancho de banda.

Los **servicios proporcionados al nivel de aplicación** son **orientado a conexión, confiable** (TCP), y **sin conexión, no confiable** (UDP).

2.2 Multiplexión y demultiplexión

Es una extensión del servicio de entrega de host a host que proporciona el nivel de red a un servicio de entrega de proceso a proceso para el nivel de aplicación. El nivel de transporte tiene la responsabilidad de entregar los segmentos recibidos al proceso correcto.

La **multiplexión** consiste en obtener información de los distintos sockets, crear los segmentos y pasarlos al nivel de red.

La **demultiplexión** consiste en entregar los segmentos procedentes del nivel de red a los sockets apropiados.

2.2.1 Direccionamiento de procesos

Cada paquete IP recibido por un host tiene direcciones IP de origen (S) y de destino (D). Cada paquete IP transporta un segmento TCP o UDP. Cada segmento tiene números de puerto origen y de puerto destino. El host utiliza las direcciones IP y los números de puerto para entregar el segmento a socket apropiado. UDP (IP D, Port D), TCP (IP D, Port D, IP S, Port S).

2.3 Protocolo UDP

Protocolo del nivel de transporte que solo incorpora las funciones de multiplexión/demultiplexión y detección de errores. Proporciona servicio best effort del nivel de transporte, lo que significa que la entrefa no está garantizada, ni el orden de entrega tampoco. Es un protocolo sin conexión, es decir, no hay negociación alguna entre emisor y receptor, y cada segmento UDP se trata de forma independiente.

Se trata de un protocolo multipunto, un proceso puede enviar y recibir información a o desde otros procesos con el mismo socket.

2.3.1 Campos del segmento UDP

Está formado por dos partes, que son una cabecera de controlo y los datos del nivel de aplicación.

Campos de la cabecera: puertos del proceso emisor y del proceso receptor del segmento. Longitud del segmento UDP incluyendo la cabecera. Checksum para detección de errores.

Detección de errores:

- **Cálculo del checksum:** tratar los contenidos del segmento como una secuencia de enteros de 16 bits. El checksum es la suma en complemento a 1 de todos los enteros de l secuencia. El emisor incluye el checksum calculado en el campo correspondiente del segmento.
- **Comprobación del checksum:** el receptor calcula el checksum de la misma forma, si ambos coinciden, no hubo errores durante la transmisión del mensaje, en otro caso, el segmento se descarta.

Razones para usar UDP frente a TCP: la aplicación tiene más control acerca de cómo se envía la información. No hay control de flujo ni recuperación de errores, lo que evita la retransmisión de segmentos perdidos o erróneos. Tampoco hay control de la congestión, por lo que se puede enviar a la velocidad deseada.

Se elimina el retraso asociado a establecer la conexión.

No se necesita guardar el estado de la conexión. Normalmente un servidor de aplicaciones podrá atender a más clientes si usa UDP que con TCP.

La cabecera del segmento es menor, y por tanto la eficiencia mayor.

UDP en la práctica: es habitual su uso para aplicaciones multimedia en tiempo real o que usan streaming. También se usa para DNS (Domain Name Service), DHCP (Dynamic Host Configuration Protocol), SNMP (Simple Network Management Protocol) o RIP (Routing Information Protocol).

En caso de que se requiera un servicio de transmisión confiable basado en UDP, los mecanismos para garantizarla deben incluirse en el nivel de aplicación.

2.4 Principios de la comunicación confiable

Un protocolo confiable debe proveer un servicio que garantice que ningún bit será modificado o se perderá, y que aseguro que todos los bits se entregarán en el destino en el mismo orden en que fueron enviados, considerando que la capa inferior es un canal punto a punto no confiable.

Protocolo rdt (reliable data transfer)

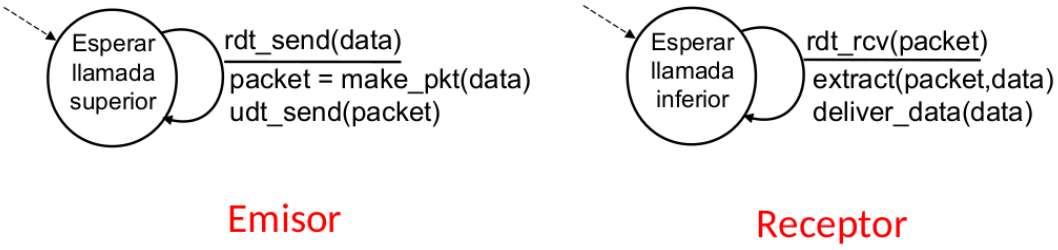
2.4.1 Primitivas de envío y recepción

- **rdt_send():** usada por la capa superior para que los datos sean entregados a la capa superior del receptor.
- **udt_send():** usada por rdt para enviar un segmento por el canal no confiable al receptor.
- **rdt_rcv():** usada por la capa inferior cuando llega un segmento por el canal no confiable al receptor.
- **deliver_data():** usada por rdt para entregar datos a loa aplicación.

2.4.2 rdt 1.0: Canal confiable

Supongamos que el canal subyacente es confiable, no hay errores de bits y no hay pérdida de segmentos.

Basta que el emisor envíe datos a través del canal subyacente y que el receptor los lea.



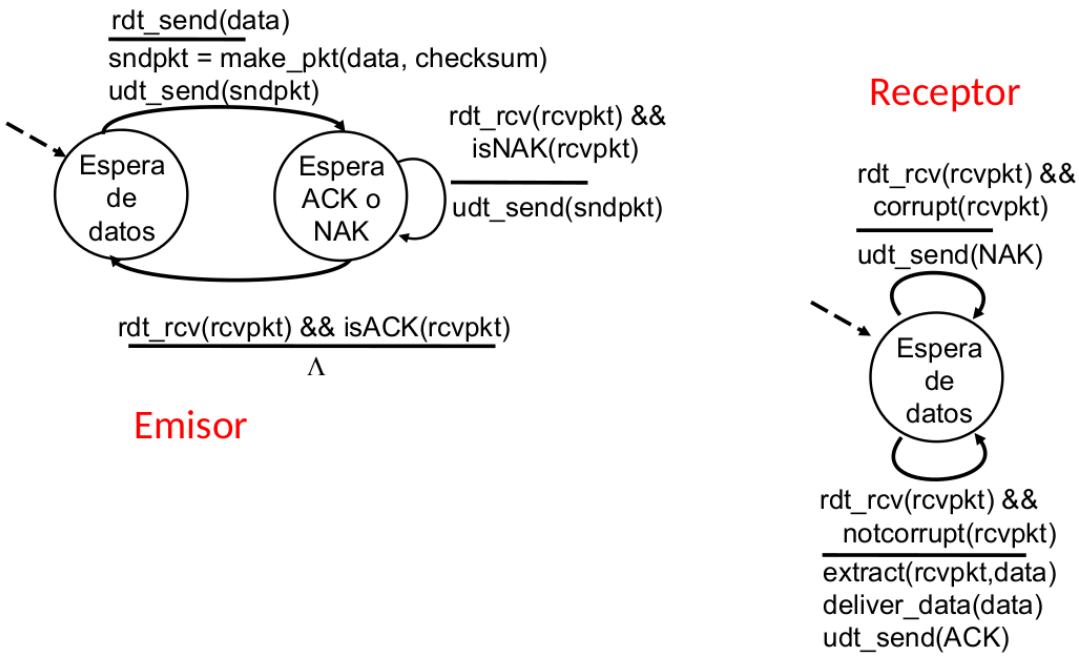
2.4.3 rdt 2.0: Canal con errores de bits

Ahora el canal subyacente puede alterar los bits del segmento, pero no hay pérdida de segmentos.

Utilizaremos un mecanismo de checksum para detectar esto.

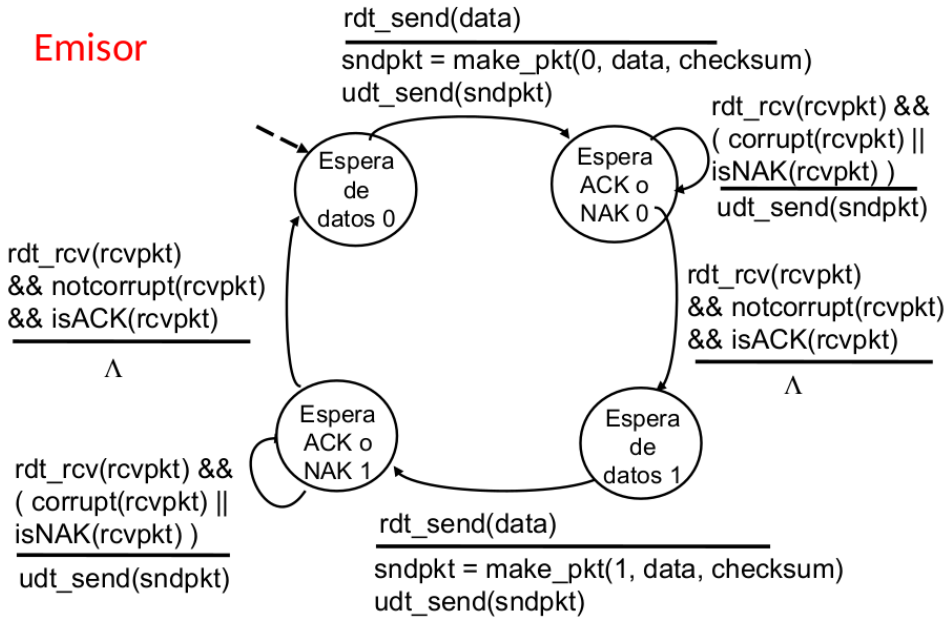
Mecanismos básicos para recuperación de errores:

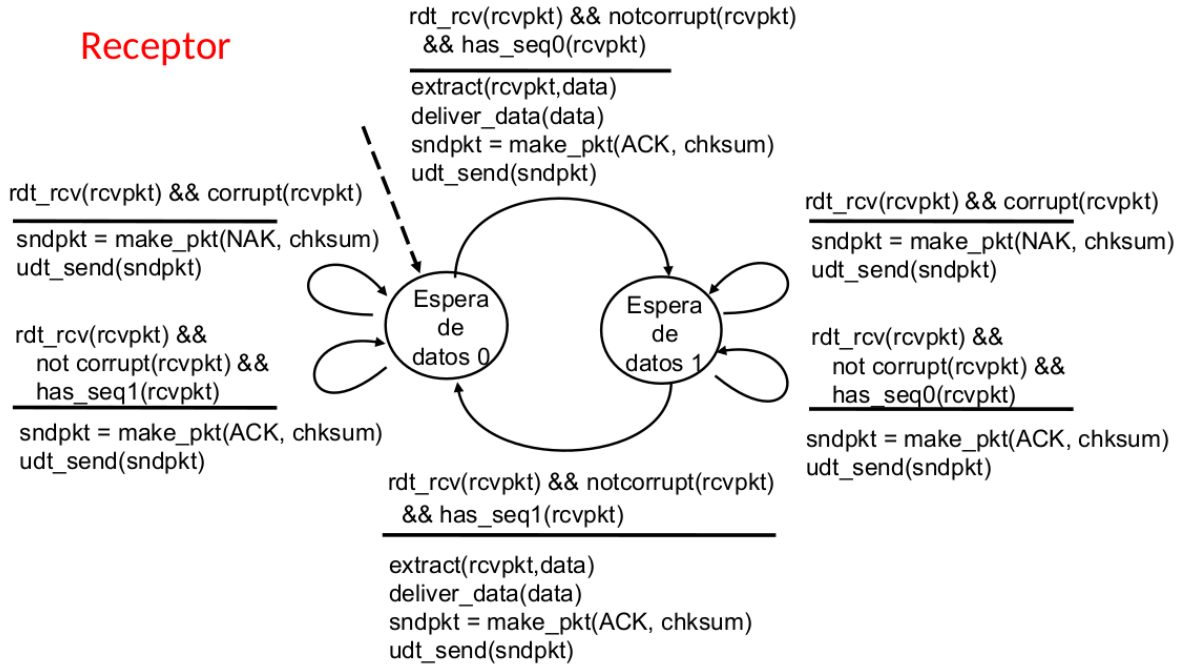
- **ACKs (Asentimientos):** el receptor indica explícitamente que el segmento se recibió correctamente. El emisor no enviará otro segmento hasta recibir un ACK.
- **NAKs (Rechazos):** el receptor indica explícitamente que el segmento contenía errores. El emisor retransmite el mismo segmento si recibe un NAK.



rdt 2.0 tiene un fallo bastante grave, pues si un ACK o un NAK se corrompen, el emisor no sabía realmente qué pasó en el receptor, por lo que el emisor no puede retransmitir un segmento porque el receptor lo podría procesar aún siendo un duplicado.

Hace falta un mecanismo adicional (rtd 2.1), en el que el emisor añadirá un número de secuencia a cada segmento, transmitirá de nuevo el segmento si el ACK o el NAK se han visto afectados por un error, y el receptor descartará los segmentos duplicados.

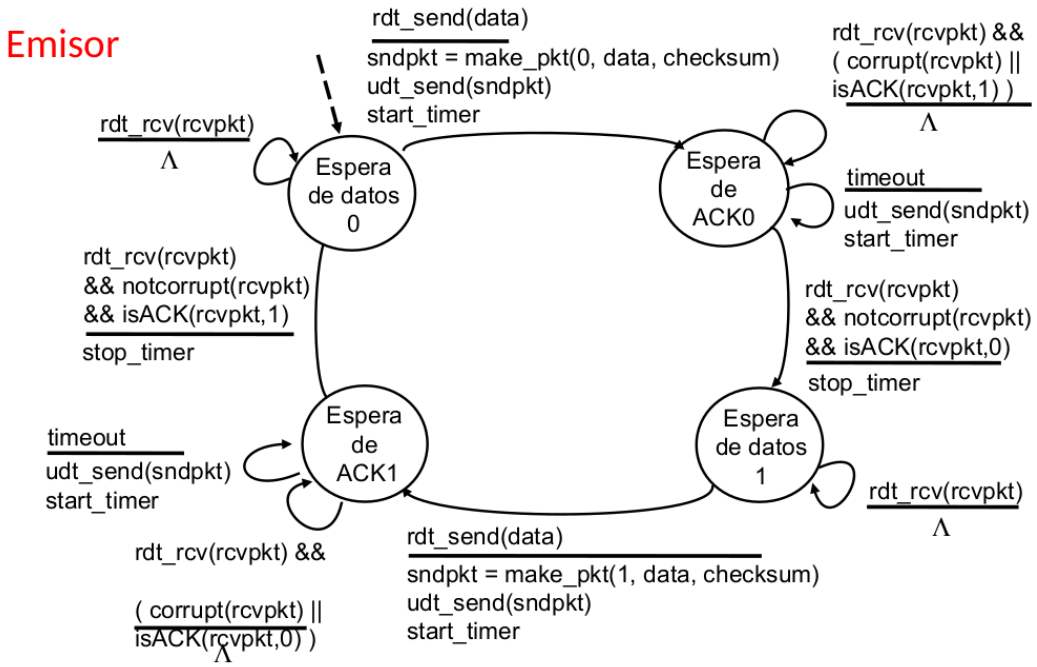




2.4.4 rtd 3.0: Canal con errores y pérdidas de bits

El canal subyacente también puede perder segmentos. Ahora, el checksum, los números de secuencia, los ACKs y las retransmisiones no son suficientes.

Necesitamos otro mecanismo adicional: el emisor espera durante un tiempo razonable el ACK (timeout), el segmento se retransmite si no llega el ACK durante ese tiempo, si los datos o el ACK solo se retrasan, la retransmisión generará duplicados que pueden detectarse mediante los números de secuencia de los segmentos.



Eficiencia de rdt 3.0 sin errores

Es un protocolo de parada y espera (stop and wait), lo que quiere decir que el emisor espera una confirmación por cada segmento transmitido y el siguiente segmento se envía solo cuando se recibe su confirmación. Así, el tiempo total para transmitir un segmento y su confirmación es:

$$T = t_{prop} + t_{seg} + t_{proc} + t_{prop} + t_{ack} + t_{proc}$$

Siendo t_{prop} : tiempo de propagación, t_{seg} : tiempo de transmisión de un segmento, t_{proc} : tiempo de procesamiento de un segmento o ACK, t_{ack} : tiempo de retransmisión de un ACK.

Tiene como ventaja la simplicidad, pues cada segmento se transmite y confirma individualmente. Y como desventaja la ineficiencia, por la espera entre sucesivos envíos.

Se define **utilización o eficiencia del protocolo** como:

$$U = \frac{t_{info}}{T} = \frac{t_{info}}{2t_{prop} + 2t_{proc} + t_{seg} + t_{ack}}$$

$t_{prop} = \frac{d}{V_{prop}}$, d=distancia del enlace, V_{prop} =velocidad de propagación

$t_{seg} = \frac{L}{V_{trans}}$, L=longitud del segmento, V_{trans} =velocidad de transmisión

Si se conoce el tamaño de la cabecera del protocolo (h), entonces t_{info} es el tiempo necesario para transmitir solo los datos del segmento (L-h), sin la cabecera. Si no se conoce, entonces $t_{info} = t_{seg}$.

2.4.5 Uso de técnicas de ventana deslizante

Protocolo de ventana deslizante (sliding-window): el emisor puede enviar varios segmentos antes de recibir una confirmación, lo que permite aprovechar más eficientemente el canal. El emisor guarda copias de los segmentos enviados hasta que recibe el ACK correspondiente. El receptor puede confirmar la recepción de uno o más segmentos en cualquier momento mediante un ACK.

-Mecanismo de control de flujo: el número máximo de segmentos enviados pendientes de confirmación se conoce como ventana. Esta limitación evita que un emisor rápido inunde a un receptor lento.

Este protocolo requiere un esquema de numeración de los datos y los ACKs para realizar un seguimieento de los segmentos enviados y recibidos. Cada segmento de datos incluye un número de secuencia y cada ACK debe incluir información acerca de cuántos segmentos está confirmando.

El emisor también dispone de uno o más temporizadores para recuperarse de las pérdidas de segmentos.

Eficiencia de la ventana deslizante sin errores

$$U = \frac{N \cdot t_{info}}{T}$$

donde N es el número de segmentos que se pueden enviar sin esperar confirmación.

2.5 Protocolo TCP

Ofrece un servicio confiable del nivel de transporte, la información no puede perderse y siempre se entrega en orden al nivel de aplicación.

Es un protocolo orientado a conexión, en el que el emisor inicia una negociación con el receptor para establecer la conexión. Es punto a punto con transmisión full-dúplex, con un solo emisor y un solo receptor (IP D, Port D, IP S, Port S), en el que el flujo de información es bidireccional en cada conexión.

El control de flujo y recuperación de errores están basados en técnicas de ventana deslizante. Solo se implementa en sistemas finales.

Campos del segmento TCP:

Está formado por dos partes, que son la **cabecera de control**, y los **datos del nivel de aplicación.**

Hay una longitud máxima del segmento, MSS (Maximum Segment Size), que se define como el tamaño máximo del campo de datos y está condicionado por las capas inferiores. Si los datos de la aplicación no caben en un segmento se generan varios.

Cabecera:

- Puertos del proceso emisor y del receptor.
- Número de secuencia y número de confirmación.
- Head Len indica la longitud de la cabecera en palabras de 32 bits.
- Flags (ACK confirmación, SYN establecer conexión, RST restaurar conexión, FIN cerrar conexión).
- La ventana del receptor se utiliza para control de flujo.
- Checksum.

2.5.1 Conexiones TCP

Tanto el emisor como el receptor deben establecer una conexión antes de comenzar el intercambio de datos procedentes del nivel de aplicación. El propósito de este establecimiento es inicializar los parámetros relativos a al recuperación de errores, como son los campos de número de secuencia y de confirmación, inicializar los parámetros relativos al control de flujo, o sea, el valor del campo Ventana del receptor en ambos sentidos, y reservar buffer para la ventana deslizante en ambos sentidos.

El **establecimiento** se lleva a cabo en tres fases:

1. El cliente envía un segmento SYN al servidor, en el que especifica el número de secuencia inicial del cliente y no incluye datos.
2. El servidor recibe el SYN y recibe con un SYN ACK, reserva los buffers necesarios y especifica el número de secuencia inicial del servidor.
3. El cliente recibe el SYN ACK y responde con ACK, reserva los buffers necesarios, y ya puede incluir datos para el servidor.

El **cierre** consiste en cuatro pasos:

1. El cliente envía un segmento FIN al servidor.
2. El servidor recibe el FIN, cierra la conexión, responde con ACK, y envía un FIN.
3. El cliente recibe el FIN y responde con un ACK. El cliente espera algún tiempo antes de cerrar la conexión, si el ACK se pierde, el servidor enviaría de nuevo un FIN.
4. El servidor recibe el ACK y cierra la conexión.

Tanto el emisor como el receptor liberan todos los recursos asociados a la conexión cuando la cierran.

2.5.2 Números de secuencia y confirmaciones

TCP considera los datos como un flujo de bytes ordenados. Los números de secuencia están relacionados con los bytes transmitidos, no con el número de segmentos. El número de secuencia de un segmento corresponde al primer byte de dicho segmento, por lo que el número de secuencia del siguiente segmento depende del número de bytes transmitidos anteriormente.

Los números de confirmación también están relacionados con los bytes recibidos. El número de confirmación de un segmento indica el número de secuencia del byte que se está esperando. Las confirmaciones pueden ser acumulativas, o sea, se pueden confirmar varios segmentos simultáneamente.

Si se recibe un segmento fuera de orden, el receptor puede optar por descartarlo o almacenarlo en espera de los anteriores.

2.5.3 Estimación del temporizador

Debe ser mayor que el RTT (Round-Trip Time, el tiempo de ida y vuelta) necesario para que un segmento pueda llegar a su destino y se reciba su confirmación. El RTT varía en función del camino seguido por los paquetes.

Si fuera demasiado bajo, se podrían producir retransmisiones innecesarias y si fuera demasiado alto se reaccionaría lentamente ante las pérdidas de segmentos.

TCP lleva a cabo una estimación constante del RTT. Se mide el tiempo transcurrido desde que se envía un paquete hasta que se recibe su ACK. Como los valores obtenidos fluctuan, se calcula la media teniendo en cuenta los valores recientes.

2.5.4 Funcionamiento del emisor

1. Al recibir datos desde el nivel de aplicación se crea un segmento con el número de secuencia apropiado y se envía. Se inicia el temporizador si está detenido.
2. Si expira el temporizador, se retransmite solo el segmento asociado al temporizador y se reinicia este.
3. Si se recibe un ACK:

- Si se están confirmando segmentos aún no confirmados se actualiza el buffer de emisión de acuerdo con la confirmación y se reinicia el temporizador si aún quedan segmentos pendientes de confirmación.

- Si se trata de un ACK repetido por 4ª vez se asume que el segmento se ha perdido y se reenvía sin esperar a que venza el temporizador.

También existen ACKs selectivos, aunque su uso es opcional.

2.5.5 Control de flujo

El buffer de recepción de una conexión TCP es finito y la aplicación que lee el buffer puede ser lenta.

El control de flujo sincroniza la velocidad de emisión con la frecuencia de lectura del buffer de recepción.

El receptor informa del espacio disponible en el buffer mediante el campo **Ventana del receptor**.

El emisor limita la cantidad de bytes sin confirmar evitando así el desbordamiento de dicho buffer.

3 El nivel de red

3.1 Introducción

El **objetivo** del nivel de red es proporcionar un servicio de encaminamiento de paquetes entre hosts a través de la red. Este nivel involucra a hosts y routers.

El emisor encapsula los segmentos en paquetes.

El router almacena el paquete, examina su cabecera y lo reenvía.

El receptor entrega los segmentos al nivel de transporte.

Las **funciones** del nivel de red son transportar paquetes desde un host origen hasta un host destino a través de la red, determinar la trayectoria más apropiada para los paquetes a través de la red (depende de la topología, el algoritmo de encaminamiento y es necesario un esquema de direccionamiento lógico uniforme), evitar la congestión de enlaces y equipos de interconexión, interconectar subredes tecnológicamente distintas y aislar el nivel de transporte de las tecnologías de las subredes que atraviesa el paquete.

3.1.1 Calidad de servicio en el nivel de red

Define las características del servicio de transporte de paquetes entre un host origen y un host destino.

Se consideran servicios deseables para paquetes inidividuales la entrega garantizada y con un retraso máximo acotado.

Son servicios deseables para flujos de paquetes la entrega en orden, un ancho de banda mínimo garantizado, una fluctuación del retardo máximo entre paquetes acotada y servicios de seguridad.

Internet proporciona por defecto un único tipo de servicio, el best effort, o sea, no se garantiza ningún servicio.

3.1.2 Servicios y protocolos del nivel de red

Los protocolos utilizan el servicio de transmisión de tramas entre nodos conectados directamente proporcionado por el nivel de enlace.

Algunos protocolos de red disponibles en internet son IP (Internet Protocol), con entrega no garantizada y posiblemente desordenada de los paquetes, sin garantías de latencia ni de ancho de banda, y ATM (Asynchronous Transfer Mode), que ofrece varios niveles de calidad de servicio.

Los servicios proporcionados al nivel de transporte pueden ser orientados a conexión y confiables (subred de circuitos virtuales), o sin conexión y no confiables(subred de paquetes).

3.2 Organización interna de la red

Hay dos categorías principales de organización: las **redes de datagramas** (proporcionan un servicio de red sin conexión) y las **redes de circuitos virtuales** (proporcionan un servicio de red orientado a conexión).

Los servicios del nivel de red son análogos a los servicios del nivel de transporte pero con ciertas diferencias, como que el servicio es host a host, no proceso a proceso; no hay elección, cada red implementa uno u otro; y la implementaciń del servicio se realiza en el núcleo de la red, no en los sistemas finales.

3.2.1 Circuitos virtuales

Establecimiento del circuito virtual:

1. Se establece una ruta fija entre el host origen y el host destino para todos los paquetes.
2. El encaminamiento se realiza una sola vez.
3. Cada router reserva ciertos recursos internos para mantener el estado de todos los circuitos virtuales que pasan por él.
4. Además, cada router también puede dedicar algunos recursos en los puertos que atraviesa el circuito virtual en exclusiva.

Flujo de paquetes entre host origen y destino: todos los paquetes siguen la misma ruta. Para ello, cada paquete contiene un identificador de circuito virtual. Cada router mantiene una tabla de reenvío que asocia (Puerto de entrada, Id CV) con (Puerto de salida, Id CV). Los paquetes son modificados en cada router, pues los identificadores tienen un significado local.

Liberación del circuito virtual: se eliminan las entradas de las tablas de reenvío y los recursos asociados al circuito virtual en todos los routers que atraviesa.

3.2.2 Red de datagramas

Cada paquete se encamina de forma independiente, de forma que no se establece una ruta fija entre cada par de hosts, sino que cada paquete contiene la dirección del host origen y la dirección del host destino, y cada router mantiene una tabla de encaminamiento que asocia un puerto de salida a cada posible dirección de destino. Esta tabla no es estática, sino que puede variar con la topología, los fallos en la red,...

Tampoco se almacena información asociada a los flujos de datagramas transportados en los routers.

Comparación entre datagramas y CVs		
Función	**Datagramas**	**Circuitos Virtuales**
Establecimiento CV	Innecesario	Requerido
Direccionamiento	Dirección completa de origen y destino en cada paquete	Identificador de canal virtual en cada paquete
Encaminamiento	Cada paquete de forma independiente	Todos los paquetes siguen la misma ruta
Información estado (router)	Innecesario	Cada CV requiere una entrada en la tabla de reenvío
Liberación CV	Innecesario	Requerida
Control de errores	Los paquetes erróneos se descartan	Factible
Control de congestión	Difícil	Factible
Calidad de servicio	Difícil	Factible
Tolerancia a fallos (router)	Posible si existen rutas alternativas entre host origen y destino	Imposible, si cae un nodo del CV cae todo el CV
Complejidad	Mayor en los hosts	Mayor en los routers

3.3 Protocolo IP (Internet Protocol)

Diseñado para la interconexión de LANs, subredes o sistemas autónomos mediante la retransmisión de datagramas desde el host origen hasta el host destino

3.3.1 Campos del paquete IP

- VER: versión
- HLEN: longitud de la cabecera en múltiplos de 32 bits
- DS (Differential Services): para diferenciar el tipo de datos
- Total Length: hasta 65535 B
- Time To Live (TTL): tiempo de vida del paquete en saltos, se le resta uno en cada router, y si es 0 el paquete se descarta, informando con un paquete ICMP (Time Exceeded)
- Protocol: indica el protocolo de transporte usado
- Header Checksum: suma de comprobación de la cabecera
- Direcciones IP de origen y de destino
- Opciones: no suelen usarse

3.3.2 Fundamentos del direccionamiento

Interfaces:

Un host puede estar conectado a distintas redes. La conexión entre un host y un medio física recibe el nombre de interfaz.

Un router tiene tantas interfaces como enlaces físicos a los que esté conectado. El protocolo IP requiere que cadaa interfaz disponga de su propia dirección IP, por tanto, debe pensarse en una dirección IP como un identificador de una interfaz, y no del equipo al cual pertenece la interfaz.

Direccionamiento IP:

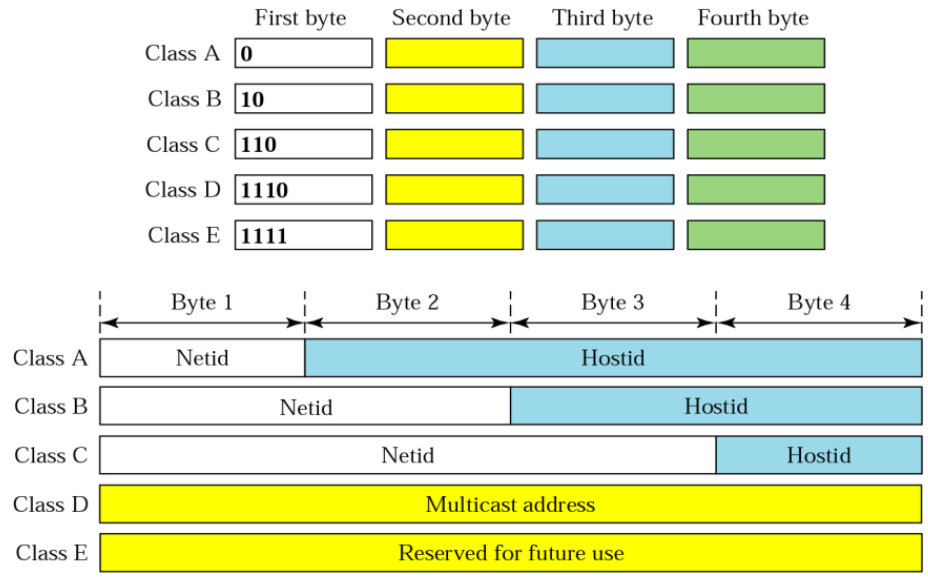
Cada interfaz de red tiene asignada una dirección IP de 32 bits, que suele expresarse como 4 números entre 0 y 255 separados por puntos. Las direcciones IP públicas son únicas, son asignadas por el ICANN (Internet Corporation for Assigned Names and Numbers).

Una dirección IP se compone de dos partes: la **dirección de red** (netid) y la **dirección de host** (hostid).

Hay direcciones especiales reservadas, que no se usan para hosts, como son la **dirección de red** (hostid es 0s) y la **dirección de broadcast** (hostid es 1s).

Puede usarse el **direccionamiento basado en clases** (classful addressing), que tiene las clases:

– Clases de direcciones:



Sin embargo, el **direccionamiento CIDR** (Classless InterDomain Routing) permite un mayor aprovechamiento del espacio de direcciones IP. En este esquema, cada dirección IP se expresa como a.b.c.d/x siendo x el número de bits de la máscara de red.

Con CIDR, los routers deben almacenar también la máscara de red porque no es posible deducirla de la clase de las direcciones.

3.3.3 Asignación de direcciones IP

La configuración de un host conta de tres valores principales, que son la dirección IP del host, la máscara de subred y la dirección IP de un router (router por defecto o gateway).

La especificación de estos valores puede realziarse mediante una configuración manual hecha por un administrador o mediante **DHCP** (Dynamic Host Configuration Protocol).

Asignación de direcciones mediante DHCP:

DHCP es un protocolo de configuración dinámica de hosts que automatiza la asignación de los valores TCP/IP desde un servidor DHCP. El administrador puede especificar parámetros de TCP/IP globales y específicos de subredes de forma centralizada en el servidor. La mayoría de los router pueden reenviar als solicitudes de configuración de DHCP. No es necesario disponer de servidores DHCP en cada subred.

3.3.4 Enrutamiento IP entre dos hosts

Si dos hosts se encuentran en la misma subred, pueden comunicarse directamente.

Si dos hosts no se encuentran en la misma subred, el host origen envía el paquete al router por defecto. Todos los equipos deben saber la dirección IP del router por defecto al que enviarán todos los paquetes destinados a una subred diferente a la que encuentran. La dirección IP de destino del paquete es la del host destino.

Cuanto un router recibe una trama, extrae el paquete IP y lo procesa, si la dirección IP de destino del paquete es distinta a la suya, reenviará el paquete en base a su tabla de encaminamiento.

Los paquetes pasan de un router a otro hasta llegar al que está conectado directamente a la subred destino.

3.3.5 NAT: Network Address Translation

La necesidad de conectar un número variable de dispositivos de una misma red local a Internet cuando solo se dispone de una única IP pública hace necesaria la búsqueda de una solución, el NAT.

El ISP no proporciona un rango de direcciones sino solo una IP para todos los dispositivos de la red local, ya que 32 bits no son suficientes para asignar direcciones IP públicas a todas las interfaces de red de internet.

Se pueden agregar nuevos dispositivos y/o modificar las direcciones IP de los dispositivos de la red local de manera transparente, se puede cambiar de ISP sin cambiar las direcciones IP de los dispositivos de la red local.

Los dispositivos de la red local no son direccionables, es decir, visibles desde Internet (enmascaramiento).

Implementación de NAT: el router actúa como traductor de direcciones y puertos entre la red Internet y la red de área local. Para los datagramas salientes, reemplaza el par (IP origen, puerto X) por (IP pública, puerto Y), de forma que los clientes/servidores remotos responderán usando el par (IP pública, puerto Y) como dirección IP y puerto destino.

Además, almacena en la tabla de traducciones NAT cada una de las asociaciones entre direcciones junto a los correspondientes puertos.

Para los paquetes entrantes, sustituye la dirección de destino y el puerto de destino por los correspondientes valores guardados en la tabla de traducciones NAT.

Los dispositivos de la red de área local pueden utilziar los siguientes rangos de IPs falsas: 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16.

169.254.9.9/16 se utiliza en ausencia de otro mecanismo de asignación de direcciones (auto IP).

3.3.6 NAT inverso

¿Qué sucede si un cliente quiere conectarse a un servidor que se ejecuta en un host con IP privada? En principio no puede, pues la única dirección visible desde internet es la dirección pública.

Para solucionar esto puede reservarse algún puerto del router para ese servidor, de forma que cualquier paquete que llegue a ese puerto, se redirija al servidor. Sería algo así como una entrada permanente en la tabla NAT de traducciones.

3.3.7 Protocolo ICMP (Internet Control Message Protocol)

IP puede fallar al intentar entregar un paquete, pero no permite al emisor detectar estos problemas ni conocer el estado de la red. ICMP es un protocolo diseñado para informar a un host de posibles errores o del estado de la red. Los paquetes ICMP viajan detro de paquetes IP pero su destino es la capa de red del host origen. El identificador de protocolo para el paquete IP es 1. El nivel de red del receptor puede informar a los niveles superiores para que tomen medidas correctivas.

Tipos de paquetes ICMP:

- **Destination Unreachable (Type=3):** puede ser Net Unreachable (Code=0), Host Unreachable (Code=1), Protocol Unreachable (Code=2), Port Unreachable (Code=3) o Fragmentation needed and DF set (Code=4).
- **Redirect (Type=5)**
- **Echo Request (Type=8) / Reply (Type=0):** identifier contiene el identificador para determinar correspondencia entre peticiones y respuestas, y sequence number es un contador. Se usa en la implementación de ping.
- **Time exceeded (Type=11):** TTL exceeded in transit (Code=0) o Fragment reassembly time exceeded (Code=1). Usado en la implementación de traceroute.

4 El nivel de enlace: Redes de área local (LAN)

4.1 Introducción

El **objetivo** del nivel de enlace es proporcionar un servicio de envío de tramas entre nodos conectados directamente. Este nivel involucra a hosts y router (nodos). Un **nodo emisor** encapsula los paquetes en tramas y las envía a través del enlace. Un **nodo receptor** entrega los paquetes al nivel de red.

Existen distintos tipos de protocolos de enlace.

Las **funciones** son proporcionar un servicio de comunicación entre nodos adyacentes sobre un único enlace físico, sincronización de tramas, identificando el comienzo y final de cada una; coordinar la comunicación, repartiendo el enlace entre varios nodos, mediante mecanismos de control de acceso al medio y esquemas de direccionamiento físico; detectar y corregir tramas erróneas; controlar el flujo y recuperar errores.

Protocolos:

- **Ethernet (802.3):** entrega no garantizada de las tramas y control de flujo opcional.
- **WiFi (802.11):** entrega garantizada de tramas (solo en el medio inalámbrico), control de flujo obligatorio de parada y espera y establecimiento de asociaciones

Ninguno ofrece garantías de latencia o ancho de banda.

El servicio proporcionado al nivel de red es sin conexión y no confiable.

4.1.1 Arquitectura IEEE 802

Define una arquitectura específica para redes LAN y PAN. Los protocolos de nivel 3 o superiores son comunes con OSI y los protocolos de niveles inferiores son específicos para LAN.

4.1.2 Funciones de IEEE 802

Las funciones de la subcapa MAC IEEE 802 son la sincronización de trama, la detección de errores y el control de acceso al medio de comunicación.

Las funciones de la capa física IEEE 802 son la generación/eliminación del preámbulo y sincronización de bit, la transmisión/recepción de bits, la especificación del medio de transmisión y la topología y la codificación/decodificación de señales.

4.2 Direccionamiento de enlace

4.2.1 Direcciones MAC

Se usan para hacer llegar una trama desde una interfaz a otra interfaz conectada al mismo enlace.

Son de 48 bits, y cada tarjeta de red tiene una dirección MAC única preasignada que se puede modificar por software.

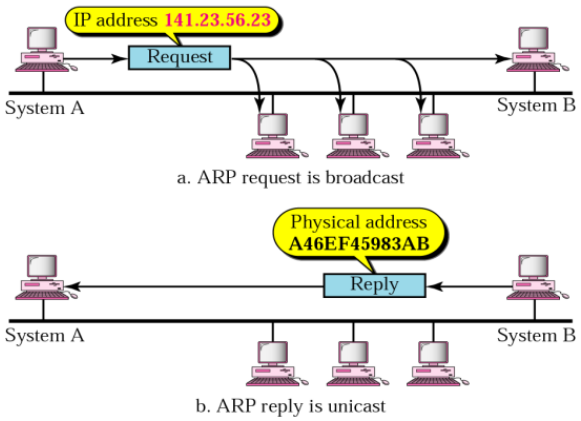
La asignación de direcciones MAC la gestiona IEEE.

4.2.2 Protocolo ARP (Address Resolution Protocol)

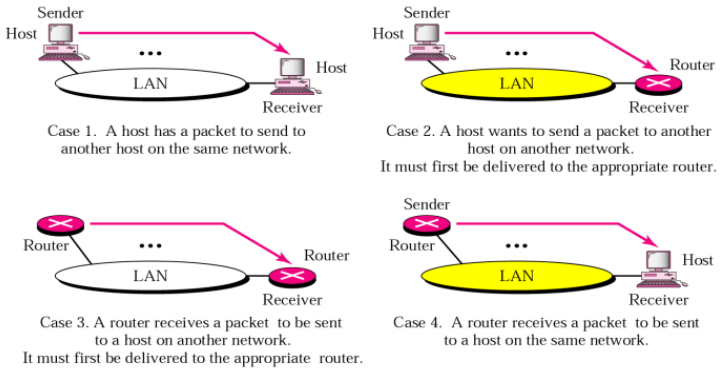
Las direcciones IP no pueden usarse para enviar paquetes porque el nivel de enlace requiere direcciones MAC.

El protocolo ARP permite a un equipo obtener la dirección MAC de otro a través de su IP.

- ARP Request (*broadcast*) ⇨ ARP Reply (*unicast*)



- Escenarios posibles de resolución de direcciones



4.3 Redes cableadas de área local

4.3.1 Tipos de redes de área local

- **LANs de ordenadores personales:** surgen con la necesidad de interconectar entre sí los PCs y los servidores. Ofrecen servicios centralizados de almacenamiento y procesamiento y compartición de recursos.
- **LANs de grandes equipos:** por la necesidad de interconectar servidores, supercomputadores y/o dispositivos de almacenamiento masivo. La velocidad de transmisión es un requerimiento crítico.
- **LANs troncales (backbone):** necesidad de interconectar varias LAN. La fiabilidad es un requerimiento crítico y presentan una mayor velocidad de transmisión que las LAN tradicionales

En todas las LAN la dispersión geográfica es limitada.

4.3.2 Control de acceso al medio

Hay dos tipos de configuración del enlace de transmisión:

Es **punto a punto** si son solo dos equipos interconectados directamente. En este caso la estación destino de una trama es conocida y el medio de transmisión está siempre disponible si es full-dúplex o debe alternarse si es semi-dúplex.

Es **multipunto** o **difusión** cuando hay dos o más equipos compartiendo medio. Hay varias alternativas a la hora de repartir el canal de transmisión:

- **Asignación estática de canal:** se divide el enlace en varios canales de manera predeterminada.
- **Asignación dinámica del canal:** manejo de colisiones, se hace por acceso aleatorio o por contienda.

La asignación estática es ineficiente en las LAN porque el número de transmisores es elevado y variable, por lo que es difícil predecir cuántos deben compartir el canal. Además, el tráfico es a ráfagas, lo que dificulta anticipar cuántos bytes transmite cada host.

El acceso aleatorio o por contienda, sin embargo, requiere mecanismos de control para gestionar el acceso al enlace y resolver los problemas derivados de las colisiones.

CSMA: (Carrier Sense Multiple Access) Permite el acceso múltiple con detección de portador. Cada estación escucha el canal antes de transmitir, si el canal está ocupado, la estación espera. Si se produce una colisión, cada estación espera un tiempo aleatorio (backoff) y vuelve a intentarlo.

- **CSMA 1-persistente:** la estación escucha el canal continuamente, si el canal está libre, la estación transmite la trama; si está ocupado, la estación espera a que quede libre y vuelve a intentarlo. Este mecanismo es bueno para redes en las que la carga no es muy elevada, puesto que evita tiempos de espera innecesarios, aunque resulta ineficiente si no pueden detectarse colisiones.
- **CSMA no persistente:** la estación escucha el canal, si está libre transmite la trama; si está ocupado, la estación espera un tiempo aleatorio y vuelve a intentarlo. Esta configuración es apropiada para canales más saturados y soporta mejor los entornos en los que no se pueden detectar colisiones.

CSMA/CD: (CSMA/Collision Detection) Con CSMA la trama se transmite por completo incluso cuando se produce una colisión. Con CSMA/CD se escucha el medio mientras se transmite la trama para detectar una posible colisión. Si se produce una colisión, cada estación detiene la transmisión de la trama en curso, transmite una señal de perturbación (jam) para asegurar que las restantes estaciones detectan la colisión y espera un tiempo aleatorio para volver a intentarlo.

4.3.3 Ethernet

- **Nivel físico:** velocidad de transmisión de 10 Mbps. Diferentes tipos de cableado, al menos de 25 MHz de ancho de banda. Normalmente configurado con topología de bus o en estrella y con codificación Manchester.

- **Nivel de enlace:** la trama Ethernet contiene un campo con la longitud y el tipo de mensaje y otro para la detección de errores. Para el control de acceso al medio se utiliza CSMA/CD 1-persistente, por la posibilidad de relleno en el campo de datos de la trama para detección de colisiones. Se usa un espacio entre tramas y un algoritmo de retroceso exponencial binario para el cálculo del backoff.

Formato de la trama Ethernet:

1. Preámbulo (7 bytes con 10101010 para sincronización de bit)
2. Guión de inicio (SFD, Start Frame Delimiter, 1 byte con 10101011)
3. Direcciones MAC destino y origen
4. Longitud/tipo
5. Relleno (padding)
6. Checksum

4.3.4 Fast Ethernet

- **Nivel físico:** velocidad de transmisión de 100 Mbps, con diferentes tipos de cableado y codificaciones. Usa la topología en estrella con conmutador y par trenzado con 125 MHz de ancho de banda.
- **Nivel de enlace:** formato de la trama y control de acceso al medio idénticos a Ethernet

La idea clave es la reducción del tiempo de bit de 100 a 10 ns. Actualmente es la Ethernet más extendida. Usa codificación **Bipolar** o codificación **por bloques 4B/5B.**

4.3.5 Gigabit Ethernet

- **Nivel físico:** velocidad de transmisión de 1000Mbps, con diferentes tipos de cableado y topología en estrella con conmutador.
- **Nivel de enlace:** formato de la trama Ethernet con extensión de portadora y control de acceso al medio de Ethernet con ráfagas de tramas.

La idea clave es la reducción del tiempo de bit de 10 a 1ns. Es una alternativa popular como LAN troncal.

4.3.6 Equipos de interconexión

Nivel físico:

- **Concentrados (hub):** retransmite la señal entrante por todas las líneas de salida. Los dominios de colisión y broadcast son únicos.

Nivel de enlace:

- **Conmutador (Switch):** retransmite la trama entrante por la línea de salida apropiada (autoaprendizaje). Hay un dominio de colisión por puerto, aunque el dominio de broadcast es único.
- **Conmutador VLAN:** es un conmutador con capacidad de crear LAN virtuales. Hay un dominio de colisión por puerto, y un dominio de broadcast por VLAN.

4.3.7 Ethernet conmutada

Está basada en el uso de par trenzado y conmutadores, lo que divide el dominio de colisión. No aumenta la velocidad, pero proporciona paralelismo. Los conmutadores pueden tener puertos con diferentes capacidades y velocidades de transmisión. Si los enlaces son full-dúplex no hay colisiones.

4.3.8 Transmisión de señales

Las señales pueden ser analógicas, si pueden tomar cualquier valor dentro de un rango, o digitales, cuando toman un número limitado de valores.

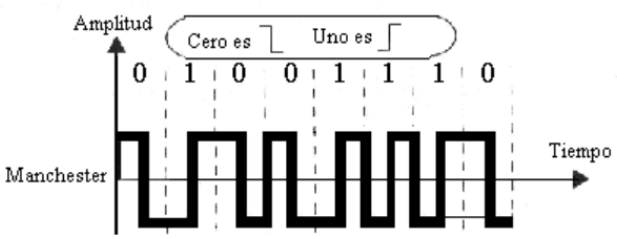
Una señal simple no transporta información, sino que debe ser manipulada introduciendo cambios identificables por el receptor, representativos de la información transmitida, para ello se usan esquemas de codificación.

- **Transmisión digital:** datos analógicos o digitales codificados en señal digital. La transmisión de datos se realiza mediante diferentes esquemas de codificación, que intentarán minimizar el ancho de banda requerido, el coste y la complejidad, facilitar la sincronización y la detección de errores, y maximizar la inmunidad frente al ruido y las interferencias.

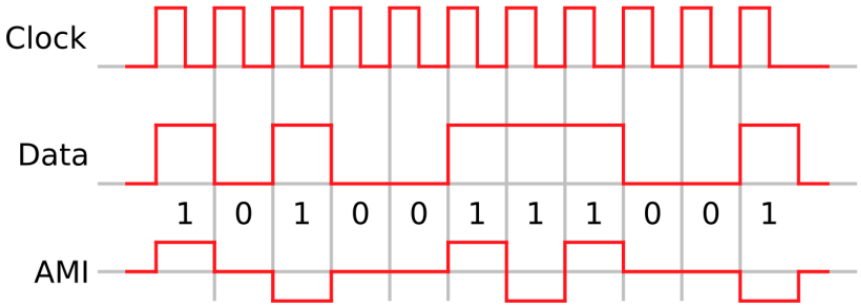
Los parámetros básicos de una señalización digital son la temporización de un bit y el nivel de señal asociado a cada valor del bit.

Y los factores que caracterizan la señalización digital son el espectro de la señal (ancho de banda requerido y presencia de componente continua), capacidad de sincronización de la señal y detección de errores en el receptor, inmunidad frente a ruido e interferencias y el coste y la complejidad.

Codificación Manchester: es una codificación polar, que funciona invirtiendo la polaridad en mitad de cada intervalo de bit. Se utliza en tecnología Ethernet a 10Mbps. Presenta como ventajas la eliminación de componente continua, la sincronización en cada bit y la detección de errores, pero necesita alta potencia.



Codificación bipolar: usa tres niveles de voltaje. La línea en estado ocioso codifica un 0, y para codificar 1's se alterna entre positivo y negativo. Elimina la componente continua, pero las secuencias largas de 0's pueden ser un problema, pues podría desincronizarse el reloj.



Codificación or bloques 4B/5B: cada 4 bits de datos se codifican con 5 bits de código. El código resultante 4B/5B se codifica con bipolar. Máximo de tres 0's por cada 5 bits de código para facilitar la sincronización y compensar la DC.

Datos	Código	Datos	Codigo
0000	11110	1000	10010
0001	01001	1001	10011
0010	10100	1010	10110
0011	10101	1011	10111
0100	01010	1100	11010
0101	01011	1101	11011
0110	01110	1110	11100
0111	01111	1111	11101

4.3.9 VLANs

Un conmutador con soporte VLAN puede definir múltiples LAN virtuales sobre la misma infraestructura. Puede agrupar puertos operando como varios conmutadores virtuales diferentes, dividiendo el dominio de broadcast.

Ventajas de las VLAN:

- **Flexibilidad:** están constituidas por distintos hosts independientemente de su situación física dentro de la LAN de una organización. Los usuarios y recursos pueden ubicarse donde más convenga.
- **Simplificación de la administración:** el cambio de ubicación de un usuario no implica reconfigurar el router, basta reconfigurar el puerto.
- **Eficiencia y seguridad:** se reduce el tráfico broadcast a lugares innecesarios. Las VLAN con más tráfico broadcast no saturan al resto.
- **Coste:** reduce el número de conmutadores y routers necesarios.

Topologías VLAN: cada VLAN identifica a una subred IP diferente. El tráfico entre VLANs pasa siempre por el router.

Si una VLAN se extiende más allá de los límites de un único conmutador, ¿cómo podemos conocer a qué VLAN pertenecen las tramas que circulan entre ambos?

La solución es IEEE 802.1Q, que define dos tipos de enlaces:

- **Trunk:** cuando se necesita distinguir a qué VLAN pertenece una trama, tagged frames.
- **Access:** cuando las tramas no son etiquetadas, pues no es necesario.

Los enlaces entre los hosts y el conmutador pueden ser trunk o access.

Los enlaces entre los routers y el conmutador deben ser trunk si pertenecen a más de una VLAN.

Para etiquetar las rtamas en 802.1Q se amplía el formato de la trama Ethernet, añadiendo el campo VID (VLAN Id), y un nuevo tipo de trama.

Conmutadores VLAN: el conmutador determina la VLAN de las tramas entrantes. Se habla de etiquetado explícito cuando el identificador está en la propia trama, y de etiquetado implícito cuando se obtiene a partir de una tabla interna con entradas <Puerto, VID>, que pueden ser estáticas (habitualmente) o dinámicas.

En función del puerto de salida el conmutador etiquetará las tramas o no.

4.4 Redes inalámbricas de área local (WLAN)

Presentan como ventajas la flexibilidad, la fácil instalación y el bajo coste, y como desventajas la menor calidad de servicio y un empeoramiento de la seguridad.

4.4.1 Arquitecturas WLAN

Los dispositivos WLAN son las **estaciones (STA)** (host con interfaz inalámbrica) y los **puntos de acceso (AP)** (posibilita la comunicación inalámbrica entre dos o más STAs.

También existen las **WLAN independientes** (IBSS, Independent Basic Service Set) que son redes ad-hoc entre estaciones, sin necesidad de APs.

Están también las **WLAN de infraestructura**, que pueden ser:

- **Basic Service Set (BSS):** grupo de STAs que utilizan el mismo AP.
- **Extended Service Set (ESS):** grupo de BSS conectados entre sí mediante un sistema de distribuciñon (DS).
- **Sistema de distribución (DS):** red de interconexión entre los BSS. Puede ser también inalámbrica (WDS, Wireless DS).

4.4.2 Control de acceso al medio inalámbrico (CSMA/CA)

En redes inalámbricas, es difícil detectar colisiones, pues la señal recibida es mucho ,ás débil que la transmitida, por lo que la comparación es compleja. Las colisiones se producen en el receptor pero no necesariamente en el emisor (estaciones ocultas).

Se intentan evitar usando CSMA/CA (CSMA/Collision Avoidance) en lugar de CSMA/CD

CSMA/Collision Avoidance: acceso múltiple con detección de portadora y prevención de colisiones. Intenta evitar las colisiones mediante dos estrategias: el espacio entre tramas y el envío no persistente.

Se envían confirmaciones para asegurar que no se produjo una colisión y que la trama fue recibida correctamente. Se utiliza en la subcapa MAC de WiFi.

4.4.3 Subcapa MAC de WiFi

Envío de paquetes unicast (CSMA/CA): la estación debe esperar DIFS antes de enviar trama. El receptor confirma que la trama se recibió correctamente (CRC) con un ACK tras esperar SIFS. En caso de error se retrnasmite la trama, es un protocolo de parada y espera. La retransmisión implica reiniciar el algoritmo.

Modo de operación en 802.11: las STAs tienen que asociarse con los puntos de acceso. Para ello, los APs envían tramas beacon periódicamente con información de su BSS. Los STAs escanean los canales buscando tramas de beacon. Seleccionancon qué AP se asocian por orden de preferencia del usuario y de mayor potencia de señal. Se autentican frente al AP elegido y se asocian a este. El AP necesita reservar recursos para mantener la conexión. A continuación pueden enviar tráfico TCP/IP.

4.4.4 Codificación analógica

Codificación basada en una señal de frecuencia constante: **portadora**. La transmisión de datos se realiza modificando parámetros de la portadora, esto se llama **modulación.**

Modulaciones de una sola componente:

- **Modulación en amplitud (ASK):** una distinta amplitud para cada valor de bit. Muy sensible a cambios de voltaje. Se usa en líneas de fibra óptica.
- **Modulación de frecuencia (FSK):** distinta frecuencia para cada valor de bit. Es menos sensible a cambios de voltaje pero limitada por al potencia. Se utiliza en tecnologías como Bluetooth 5.0.
- **Modulación de fase (PSK):** distinta fase para cada valor de bit. Las variaciones de fase son fácilmente identificables.

La **velocidad de transmisión (V_T)** es el número de bits transmitidos por unidad de tiempo.

La **velocidad de modulación (V_M)** es el número máximo de cambios por unidad de tiempo, se mide en Baudios. Cada cambio de estado podría codificar varios bits.

$V_M = \frac{1}{T_e}$, siendo T_e el tiempo de duración de cada estado.

Por otro lado, $V_T = \frac{log_2 n}{T_e} = V_M \cdot log_2 n$, siendo n el número de estados.

Modulación en varias componentes: el ancho de banda limita FSK, pero no la combinación entre ASK y PSK. Si hay X variaciones en fase, Y variaciones en amplitud (para cada fase), entonces habrá X·Y estados distintos.

Una buena elección de X e Y proporciona resistencia al ruido y robusted ante errores.

Pueden representarse gráficamente mediante diagramas de constelación