MODULO 2
TELEFONÍA IP

PARTE I

Curso EL6019
Departamento de Ingeniería Eléctrica
U. de Chile
V.2014.01

INDICE GENERAL DEL MODULO 2

Parte I

3 MODELOS OSI y TCP/IP

3.1 Introducción

3.2 Modelo OSI

3.2.1 Funciones y protocolos en Modelo OSI

3.2.2 Capas en Modelo OSI

3.2.3 Unidades de datos en las diferentes capas OSI

3.3 Modelo TCP/IP

3.3.1 Funciones y protocolos en Modelo TCP/IP

3.3.2 Capas en Modelo TCP/IP

3.3.3 Unidades de datos en las diferentes capas TCP/IP

3.3.4 Diferencias y semejanzas de TCP/IP con OSI

Parte II

Parte III

Parte IV

1 CONCEPTOS GENERALES

1.1 Conmutación de circuitos y conmutación de paquetes

Técnicas de conmutación

- **CONMUTACIÓN DE CIRCUITOS**
  - Recursos dedicados

- **CONMUTACIÓN DE PAQUETES**
  - Recursos compartidos
  - Dos variantes
    - Circuitos virtuales
    - Datagramas

Conmutación de circuitos

- **A cada comunicación se adjudica una fracción fija (un circuito) de la capacidad de cada uno de los enlaces que intervienen a lo largo de todo el trayecto.**
  - **Recursos dedicados**
  - **Trayecto fijo**
  - **Si en el momento de establecer la comunicación no hay capacidad disponible, la comunicación no puede establecerse (bloqueo) Ej., PSTN**
- **Ventajas de la conmutación de circuitos**
  - **Retardos fijos**
  - **Entrega continua garantizada**
- **Desventajas**
  - **En una comunicación establecida, los circuitos no se utilizan durante tiempos en que no se requiere transmitir información**
  - **Es ineficiente para tráfico tipo "ráfagas de datos"**
  - **La conmutación de circuitos normalmente se hace usando circuitos de velocidad de transmisión fija (64 Kbps). Dificultad para soportar velocidades de transmisión variables**

Características de la conmutación de circuitos:

- Durante el establecimiento de la comunicación se establece un circuito extremo-extremo que se utiliza durante toda la llamada para intercambiar la información entre los abonados A y B.
- Cada nodo de conmutación (central telefónica) colabora estableciendo secciones del circuito extremo-extremo.
- Las distintas secciones del circuito pueden ser de muy distintas naturalezas: par de cobre (conexión galvánica), enlace de radio FDM analógico, enlace de radio TDM digital, redes de datos en que se establece un circuito virtual …
- La existencia de un circuito dedicado a la comunicación mientras ella esté establecida, garantiza baja probabilidad de pérdida de información.

PROBLEMAS CON LA CONMUTACION DE CIRCUITOS

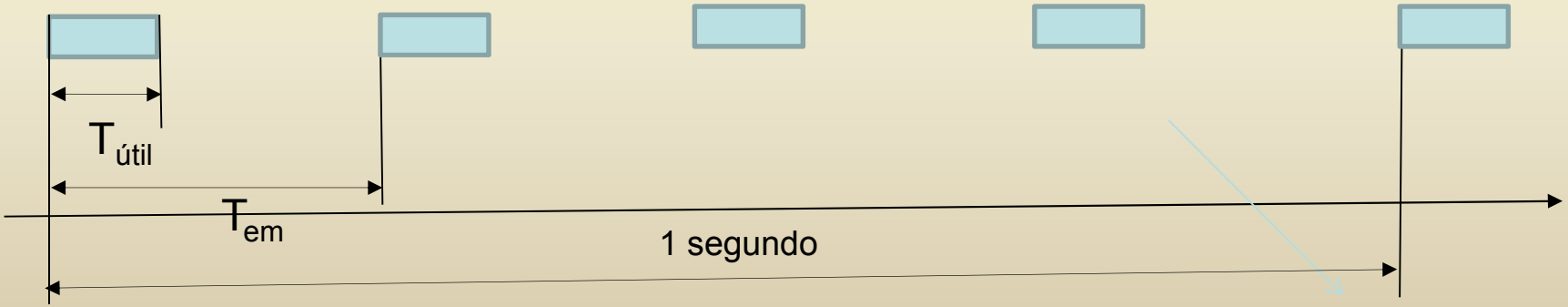
- Muchas comunicaciones de datos tiene bajo factor de uso del circuito (<< 1), al ser tipo ráfagas.

$$\text{Factor de uso} = U = \frac{T_{útil}}{T_{em}} \qquad \text{Como } \frac{1}{T_{em}} = f$$

En que f = frecuencia de los mensajes [mensajes/seg]

$$\text{Factor de uso} = U = f * T_{útil}$$

$T_{útil}$ = Tiempo de transmisión de los mensajes [seg]
T_{em} = Tiempo entre llegada de mensajes (período de los mensajes) [seg]



OTRA FORMA DE VER EL PROBLEMA

Si el canal de transmisión tiene una capacidad **C** [bits/seg] (caudal máximo), y nuestros datos se están enviando a un caudal inferior, el canal de datos se está subutilizando.

El factor de uso del canal de datos es:

$$U = \frac{\text{Caudal real de envío}}{\text{Caudal máximo que permite el canal}}$$

Al caudal máximo que permite el canal se denomina CAPACIDAD del canal, y se mide en [bits / seg.]

El caudal real de envío corresponde a la frecuencia de los mensajes multiplicada por la cantidad de bits de cada mensaje, si:

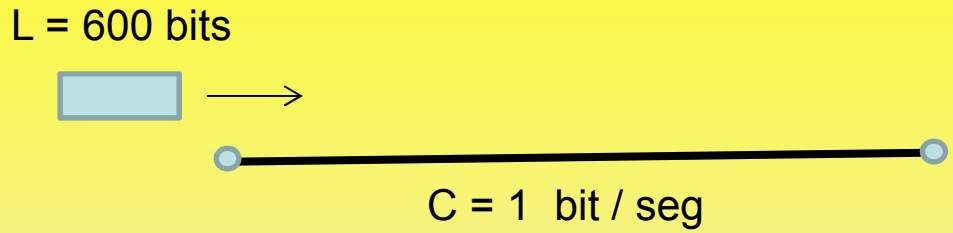
f = Frecuencia de los mensajes [mensajes / seg]
L = Cantidad de bits de cada mensaje [bits / mensaje]

El factor de uso es:

$$U = \frac{f * L}{C}$$

RETARDO QUE INTRODUCE EL CANAL DE TRANSMISIÓN

En el sencillo ejercicio que ahora veremos, se trata de transmitir en serie un mensaje de largo L = 600 bits, utilizando un canal de baja velocidad (C = 1 bit / seg)



El último bit será recibido después de los 599 anteriores.
Como en este caso para transmitir cada bit se requiere un segundo, el RETARDO = R que experimenta el mensaje (su transmisión completa) es R = 599 + 1 = 600 seg.

Si la velocidad de tx es C veces mayor que 1 bit/seg, el tiempo requerido para transmitir cada bit es $\frac{1}{C}$ y el tiempo para transmitir los L bits es $\frac{L}{C}$

Se tiene entonces que si la capacidad (o velocidad de tx.) del canal es C [bits / seg], el retardo R que experimenta un mensaje de largo L [bits] es:

$$\mathbf{R = \frac{L}{C}}\ [\text{seg.}] \quad \mathbf{[1]} \qquad \text{y como } \frac{L}{C} = \frac{U}{f} \text{ se tiene que } \quad \mathbf{U = f * R} \quad \mathbf{[2]}$$

$$R = \frac{L}{C} \text{ [seg.]}$$

El retardo que sufre un mensaje es directamente proporcional a la cantidad de bits L de éste. Ello porque el mensaje no puede ser leído en el extremo receptor sino hasta cuando se ha recibido el último bit.

Conviene entonces, para disminuir el retardo, transmitir la información en porciones pequeñas. Así nace el concepto de PAQUETIZAR los mensajes.

Por ejemplo si necesitamos transmitir un archivo extenso, conviene dicho archivo dividirlo en muchos paquetes de largo L pequeño. En el extremo receptor vamos reconstituyendo el archivo a medida que los paquetes van llegando y en muchos casos la información puede ir siendo utilizada de inmediato (ejemplo: cuando descargamos un video de la web podemos ver simultáneamente que parte del archivo hemos recibido y que parte del archivo hemos visto en la pantalla).

Sin embargo, como veremos más adelante, paquetizar tiene un costo: introduce overhead. Habrá que buscar el equilibrio de manera que la disminución del retardo no signifique un overhead inaceptable.

EN COMUNICACIONES EN TIEMPO REAL:

•La velocidad de transmisión asignada a la comunicación debe ser suficientemente grande para evitar retardos inaceptables. Esta capacidad de transmisión queda ociosa cuando no hay ráfagas. de datos a transmitir.

• Entonces, cuando los recursos de transmisión son caros con valor proporcional a la capacidad C, la conmutación de circuitos es antieconómica y poco práctica para satisfacer los requerimientos de la transmisión de ráfagas de datos.

Ejemplo de mala utilización de los canales en conmutación de circuitos

L = Longitud de los mensajes
f = Frecuencia de los mensajes [mensajes / seg]
C = Capacidad del canal (velocidad de transmisión del canal) [bps]
R = Retardo de transmisión de los mensajes = L/C [seg] (de [1])

- **C debe ser suficientemente grande para que el retardo se mantenga aceptable**
- **Tráfico de ráfagas ==> U = f * R << 1 ==> baja utilización (de [2])**

• Ejemplo Calcular C y U para el siguiente caso:

- **L = 8.000 bits**
- **f = 2 mensaje por segundo**
- **R < 0.1 seg (máximo retardo aceptado = 0,1 seg)**
- **Como R = L/C, la capacidad del canal debe ser:**

  R < 0,1 L/C < 0,1 C > L/0,1 C > 8.000/0.1 = $8*10^4$ bps
- **El factor de utilización, resulta:**

  U = f * R = 2 * 0,1 = 20%

• Con conmutación de paquetes los canales pueden ser compartidos entre varias comunicaciones (en los tiempos entre mensajes de una comunicación se transmiten mensajes de otra comunicación) con lo que se logra mucho mayor factor de utilización.

From Eytan Modiano Slide 12

Conmutación de paquetes: dos modalidades

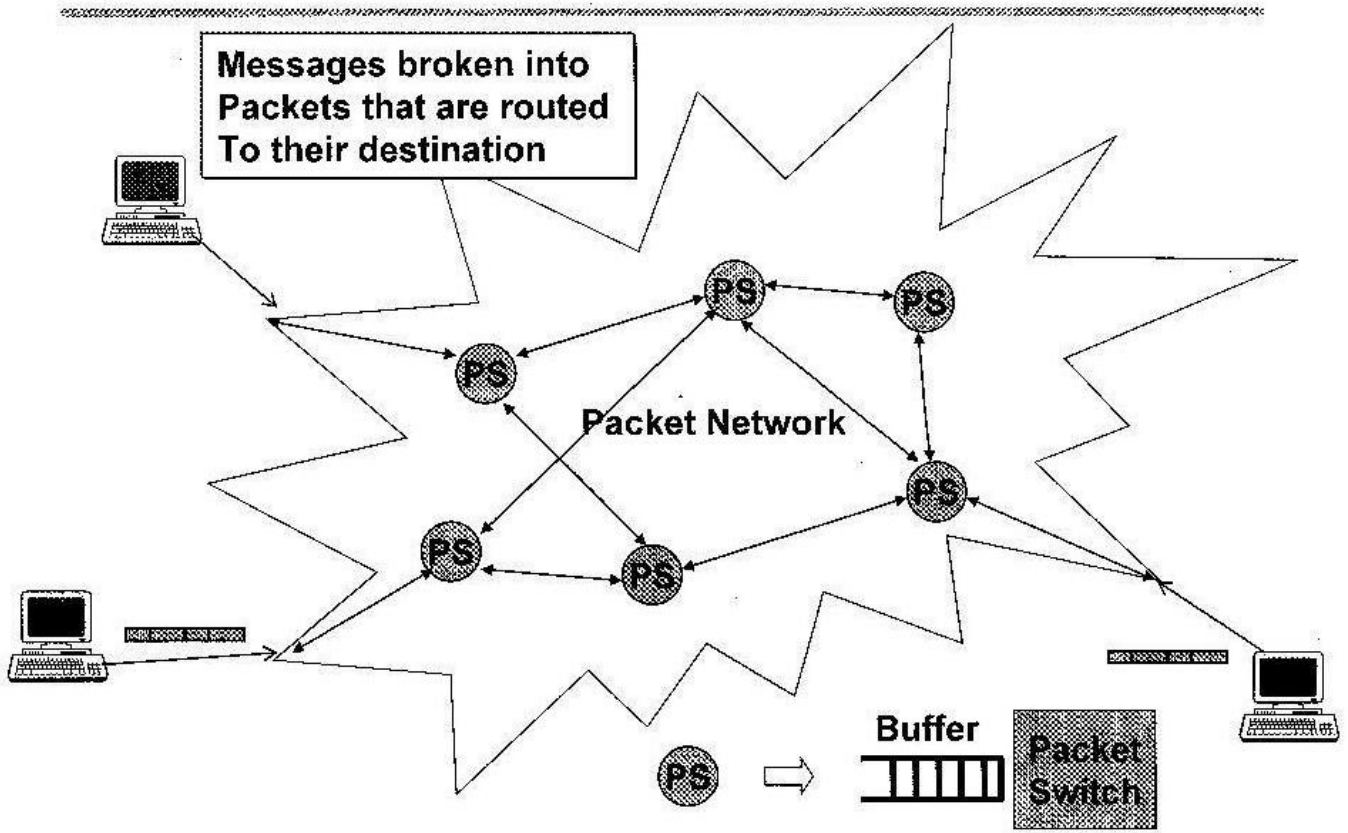
- **Conmutación de paquetes datagramas**
  - **El enrutamiento se decide para cada paquete** (Route chosen on packet-by-packet basis)
  - **Los paquetes de una misma comunicación pueden seguir diferentes rutas**
  - **Los paquetes pueden llegar al punto de recepción en orden distinto al que fueron enviados**
  - **Ejemplo conmutación paquetes datagrama: IP (Internet Protocol)**

- **Conmutación de paquetes Circuito Virtual**
  - **Todos los paquetes asociados a una comunicación siguen el mismo camino**
  - **La ruta se elige al inicio, al establecer la comunicación**
  - **Los paquetes son etiquetados con un VC# que designa la ruta**
  - **El Nº de circuito virtual es único en cada enlace, pero puede cambiar de enlace a enlace** En caso contrario, por ej. para establecer conecciones entre 1.000 nodos, números virtuales únicos obligarían a tener muchos números virtuales que deberían ser representados y almacenados en cada nodo

    Ejemplo conmutación paquetes Circuito Virtual: ATM (Asynchronous transfer mode)

Eytan Modiano Slide 14

Packet Switched Networks



Eytan Modiano
Slide 13

Características de la conmutación de paquetes:

- Se efectúa en forma distribuida en los múltiples dispositivos y computadores que conforman la red de datos IP
- Cada paquete contiene muestras de la información que intercambian los abonados A y B y además información de direccionamiento, con indicación de los dispositivos de origen y de destino, que es utilizada por los routers para encaminar los paquetes hasta sus destinos.
- Los paquetes correspondientes a la información de una misma comunicación pueden seguir caminos diferentes
- La probabilidad de que se pierda información o que llegue retrasada es mayor que en la conmutación de circuitos.

Conmutación de circuitos vs. conmutación de paquetes

- **Ventajas de la conmutación de paquetes**
  - **Eficiente para el tráfico de ráfagas de datos**
  - **Es fácil proveer variados anchos de banda con velocidades de transmisión variables**

- **Desventajas de la conmutación de paquetes**
  - **Retardos variables**
  - **Dificultad para proveer QoS garantizada (Best-effort service)**
  - **Los paquetes pueden llegar a destino desordenados**

Técnica de conmutación		Servicio de red
Conmutación de circuitos	=>	Synchronous (ej. voz)
Conmutación de paquetes	=>	Asynchronous (ej. datos)
Circuitos virtuales	=>	Orientado a la conexión
Datagramas	=>	No orientado a la conexión

De Eytan Modiano Slide 16

Red telefónica tradicional (PSTN) → Conmutación de circuitos

Redes IP → Conmutación de paquetes (*)

(*) Sin embargo debe tenerse presente que en las redes de datos también pueden establecerse circuitos virtuales, y transmitir por ellos en forma secuencial, toda la información correspondiente a una comunicación. Lo anterior significa que un circuito virtual de una red de datos puede ser parte del circuito extremo a extremo usado en una comunicación telefónica.

En este caso se tendría que en parte del circuito extremo-extremo usado para la comunicación que mayoritariamente usa la PSTN, la información se transmite en forma de paquetes por circuitos virtuales.

En la actualidad, los operadores muchas veces contratan a terceros para que les curse tráfico, los que en muchos casos hacen uso de tramos TCP/IP. De esta forma, ya no es extraño que una comunicación por la PSTN, que creemos dispone de un circuito extremo-extremo, en algún tramo no disponga de un circuito, sino que haya transmisión de paquetes tipo datagrama.

1.2 Voz sobre IP (VoIP) y Telefonía IP

Características esenciales de una comunicación VoIP

- La voz se codifica en forma de paquetes de datos (se “paquetiza”)
- Se usa una red de datos IP para transferir dichos datos

Se debe distinguir entre las expresiones “VoIP” y “Telefonía IP”:

Telefonía IP es un concepto amplio, que se preocupa de la problemática de reproducir en redes IP todos los servicios que ofrece la Red Telefónica Conmutada Pública (incluyendo, por ej., fax, ISDN, interconexión con todo tipo de redes fijas y móviles)

VoIP se refiere a la tecnología usada para transmitir voz por redes IP, sean estas redes privadas o Internet

No obstante a veces, erróneamente, ambas expresiones se usan como sinónimos.

1.3 Telefonía IP: concurrencia de conceptos

Para el estudio de la telefonía IP se requiere conocer conceptos de:

- Telefonía tradicional
- Redes de datos IP
- Nuevos conceptos, propios de la telefonía IP

Teniendo en cuenta que en los primeros capítulos del curso EL6019 ya estudiamos la telefonía tradicional, en este capítulo revisaremos principalmente los últimos dos grupos de conceptos.

1.3.1 Conceptos de telefonía tradicional

En relación a la telefonía tradicional, serán muy útiles todos los conceptos ya estudiados en este curso.

Por ahora recordemos las fases y eventos principales que se distinguen en una llamada telefónica.

En una llamada telefónica, sea ésta de telefonía tradicional o de telefonía IP, se distinguen fases:

a) Fases establecimiento y disolución de la llamada (normalmente se llama fase establecimiento a la que incluye ambas)

Corresponde a la parte de la llamada telefónica que abarca la secuencia de eventos necesarios para establecer la llamada (Call Setup) y deshacerla (Call Take Down).

b) Fase conversación

Corresponde a la parte de la llamada en que se transmite la voz, es decir en que tiene lugar la conversación telefónica. La fase conversación ocurre después de la fase Call Setup y antes de la fase Call Take Down

FASE CALLSETUP O SEÑALIZACION

1) El llamante levanta su microteléfono y recibe tono de discar

FASE CALLSETUP O SEÑALIZACION

4) La campanilla del teléfono de destino suena avisando al usuario llamado

FASE CALLSETUP O SEÑALIZACION

3) Se envían señales a través de la red con el fin de establecer un circuito para la llamada

FASE CALLSETUP O SEÑALIZACION

2) El llamante marca el número del teléfono con el que quiere comunicarse

FASE CONVERSACIÓN

5) El llamado levanta y comienza la conversación. Las señales de audio viajan en ambos sentidos a través de la red

FASE CALLSETUP (TAKEDOWN) O SEÑALIZACION

6) La conversación termina, se hace la facturación de la llamada, los circuitos y demás recursos usados durante la llamada se liberan

1.3.1.1 Fase establecimiento (Call Setup)

Durante las fases de establecimiento y disolución de la llamada se desarrollan funciones como:

- Envío de tono de invitación a marcar
- Envío de ringing,
- Envío de tono de ocupado
- Liberación

1.3.1.2 Fase conversación

Durante la fase de conversación, la voz es sometida a varios procesamientos con el objetivo de:

En el extremo emisor convertir la voz analógica en muestras digitales

Paquetizar la voz: En telefonía IP aparece la necesidad de este proceso que en telefonía tradicional no era necesario

Transmitir la voz a través de la red en formato de paquetes

Reensamblar los paquetes

En el extremo receptor volver a convertir, ahora de digital a analógico.

La conversión de análogo a digital y viceversa se realiza mediante los CODEC ubicados en ambos extremos de la comunicación

1.3.1.3 Eventos importantes durante una llamada

El llamante levanta el auricular y escucha tono de invitación a marcar

El llamante marca un número telefónico

Es invocado el protocolo de establecimiento de llamada con el fin de localizar al abonado llamado y enviarle una señal que origine ringing

El teléfono de destino suena indicando que ha llegado una llamada

El llamado levanta el auricular y se inicia la conversación bidireccional.

En telefonía IP durante la conversación las señales de audio correspondientes a la voz son codificadas como datagramas (usando CODEC) y se transmiten por la red IP en forma de paquetes

La conversación finaliza, la comunicación se da por terminada y se disuelve. Se realiza la tarificación

1.3.2 Conceptos de redes de datos

Protocolos para transmisión de datos

Son reglas precisas que regulan:

- Como construir los paquetes o bloques de datos
- Como se deben comportar los extremos que los envían y reciben

Protocolo IP

- Los protocolos para la transmisión de datos se han ido desarrollando durante los últimos 60 años
- Desde la aparición de Internet, el "Internet Protocol", o IP, se ha convertido en el más importante de todos
- IP destaca por su gran escalabilidad y adaptabilidad
- Se ha ido convirtiendo en ubicuo (está presente al mismo tiempo en todas partes)

- IP revolucionó la transmisión de datos y la forma de comunicarse
- En los últimos años la palabra “convergencia” se ha puesto de moda, abriendo grandes expectativas a la industria de las redes IP
- Convergencia: diferentes tipos de datos - voz, video y aplicaciones de datos - se transfieren usando una misma red IP

Estándares para transmisión de datos

Los organismos con mayor influencia en la creación de estándares han sido:

ITU-T “International Telecommunication Union” (ingenieros de telefonía)

IETF “Internet Engineering Task Force” (ingenieros de transmisión de datos)

El IETF ha tenido como especial preocupación los estándares IP.

Las nuevas técnicas para la transmisión de datos se someten a una rigurosa fase de pruebas, consistente en estudio, implementación y revisión, con el fin de verificar la estabilidad y robustez de ellas.

La etapa RFC (Request For Comments) es el último paso para que un borrador de estándar para Internet se transforme en estándar aprobado.

Cada componente de los Protocolos Internet TCP, UDP y RTP que discutiremos, tienen uno o más RFC que especifican su operación.

Protocolos TCP/IP

Los revisaremos en el punto 3 de estos apuntes

Protocolos telefonía IP

Los revisaremos en el punto 5 de estos apuntes

Los RFC son documentos que especifican protocolos sobre Internet. Pueden ser propuestos por cualquier persona, sin embargo solamente la IETF los reconoce como RFC después de estrictos análisis.

La página del editor RFC es http://www.rfc-editor.org/

Como ejemplo, el protocolo IP se especificó en RFC 791, en el año 1981

1.4 Componentes de la telefonía IP

Para transferir voz en forma de datos proporcionando servicio de telefonía IP, por la misma red en que hay tráfico de archivos, e-mail y web, se requiere un conjunto de componentes:

- CODEC
- Protocolos TCP/IP
- Protocolos telefonía IP
- Servidores de telefonía IP y PBX IP
- Gateways VoIP y Routers
- Teléfonos IP y Softphones

En las siguientes secciones de estos apuntes trataremos los componentes antes indicados.

2 INTRODUCCION A LOS CODEC

2.1 Descripción y objetivos de los CODEC

COmpressor / **DEC**ompressor ó **CO**der / **DEC**oder

Archivos de música, video y también correspondiente a voz de telefonía, son muy grandes como para transmitirlos y grabarlos sin previa compresión.

Los CODEC, constituidos por hardware y software o solamente por software, incluyen una serie de algoritmos e instrucciones para comprimir y descomprimir grandes archivos. El archivo correspondiente a una canción codificada con MP3, con muy buena calidad, ocupa entre 3 y 4 Mbytes, lo que es 10 veces menos que el archivo antes de descomprimirlo.

Los procesamientos de compresión conllevan pérdida de calidad, debido a que la información recuperada durante la descompresión no es exactamente igual a la original.

EJEMPLOS DE CODEC

CODEC de VIDEO: Real Video, DivX, XviD, MPEG-2,

CODEC de AUDIO: MP3, Dolby Digital AC3, OGG, WMA, Real Audio

CODEC para TELEFONIA: G.711, G.722, G.723, G.726, G.728, G.729

Para CODEC de VIDEO y AUDIO ver : www.mundodivx.com

Los CODEC más utilizados en telefonía IP por Internet son G.723.1 y G.729(A).

2.2 CODEC USADOS EN TELEFONIA

- La forma de denominar a los CODEC utilizados en telefonía es mediante el nombre correspondiente al estándar de la ITU que describe su operación. Ejemplos: CODEC G.711u (ley **μ**) y G.711a (ley a). Estos son muy populares. Convierten de análogo a digital y viceversa con relativamente alta calidad y sin compresión.
- Como siempre ocurre en el mundo digital, mayor calidad implica más bits/seg.

  Es así como los CODEC G.711 que proporcionan alta calidad, usan más ancho de banda que otros CODEC de velocidad menor pero de calidad inferior.

- Los CODEC utilizados en telefonía están constituidos por hardware y software que “muestrea” la voz analógica y la convierte en bloques de bits que el CODEC va entregando a su salida como un caudal binario de velocidad o tasa (bits/seg.), predeterminado.

- Los CODEC realizan las funciones de muestrear a intervalos regulares la señal analógica de voz, cuantizar las muestras en valores discretos, codificar, comprimir, producir bytes de 8 bits y ensamblarlos en datagramas para que sean transmitidos por la red de datos.

- La velocidad nominal a que el CODEC entrega los datagramas en su salida es uno de los factores determinantes del ancho de banda que se ocupa en la red de datos para transmitir los datagramas.

- Con el fin de ahorrar ancho de banda, algunos CODEC usados en telefonía realizan también compresión. Es así como algunos CODEC comprimen la información no transmitiendo las pausas o silencios, las que representan entre el 50% y 60% de toda la conversación telefónica. Hay docenas de CODEC disponibles, cada uno con sus propias características.

Codec G.711

También se lo denomina Pulse Code Modulation (PCM).

- Diseñado para transmitir señales de voz en el rango de frecuencias 0 - 4 KHz. Aunque la voz humana ocupa un rango de frecuencias más amplio, este rango es suficiente para satisfacer bien los requerimientos de inteligibilidad de la voz.

- A fin de capturar la información con adecuado grado de resolución, la señal analógica es muestreada al doble de la frecuencia más alta, es decir 4.000 x 2 = 8.000 veces por segundo. De esta forma PCM toma una muestra de la señal analógica cada 0,125 ms., valor que resulta de: 1 seg. / 8.000 = 0,000125 seg.

- Cada muestra se codifica en una palabra de 8 bits, por lo tanto el ancho de banda nominal es: 8.000 x 8 = 64.000 bits/seg.

- Las muestras se envían directamente, es decir la información no es comprimida

- Cuando se inventaron los CODEC G.711 la tecnología moderna de procesamiento de señales digitales (DSP) no estaba aún disponible. Los algoritmos de compresión han hecho posible proveer comunicaciones de voz inteligibles de calidad aceptable con mucho menor consumo de ancho de banda.

Otros CODEC usados para transmitir VoIP

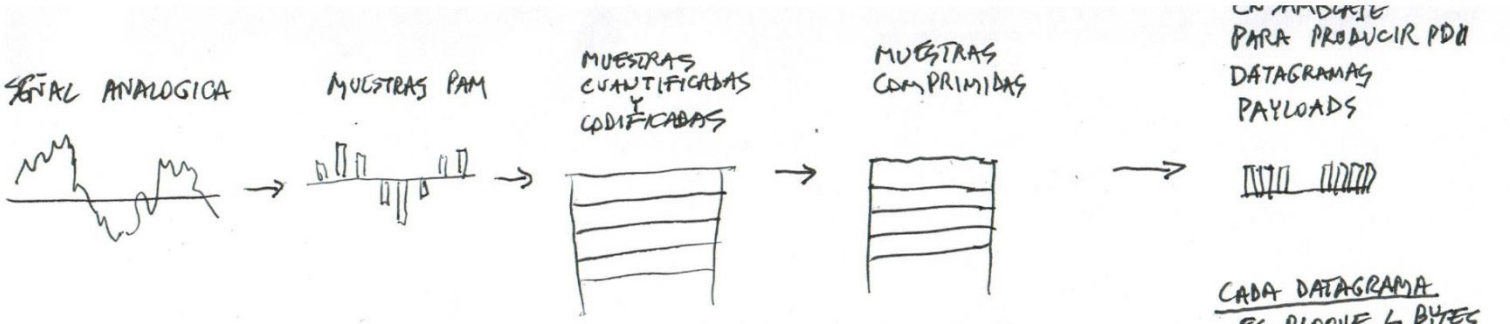
CODEC de baja velocidad como G.726, G.729 y de la familia G.723.1 requieren menos ancho de banda de la red.

Sin embargo los CODEC de baja velocidad desmejoran la calidad del audio con respecto a los CODEC de alta velocidad, debido a que comprimen los datos originales, produciéndose pérdida de información causada por los procesos de compresión.

Por otra parte, mientras menos bits se envían, el lado receptor debe hacer mayor esfuerzo para aproximarse a la reproducción del sonido original, esfuerzo que consume tiempo y por tanto produce retardos que hacen perder fidelidad.

CODEC más comunes usados en VoIP

Nombre del CODEC	Velocidad de salida nominal (V_{Codec})
G.711u	64,0 Kbps.
G.711a	64,0 Kbps.
G.726-32	32,0 Kbps.
G.729	8,0 Kbps.
G.723.1 MPMLQ	6,3 Kbps.
G.723.1 ACELP	5,3 Kbps.



CONTIENE BYTES

REDUNDANTES
INFO REPETITIVA
FACIL PREDECIR

IRRELEVATES
FREC. INAUDIBLES
SILENCIOS / RUIDO FONDO

RELEVANTES
NECESARIOS

COMPRESION

SE TRATA DE DEJAR SOLO BYTES RELEVANTES

COMPRESION
- SIN PERDIDAS REALES
  ELIMINA REDUNDANTE
- SIN PERDIDAS SUBJETIV
  ELIMINA REDUNDANTE
  IRRELEVANTE
- CON PERDIDAS
  LAS ANTERIORES Y
  PARTE DE RELEVANTE

CADA DATAGRAMA

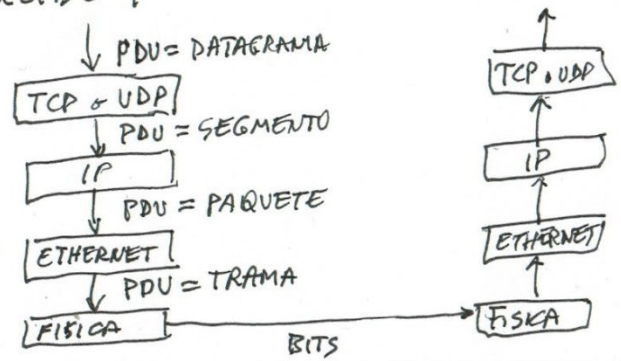
ES BLOQUE L BYTES
SE ENTREGA CADA T seg

VELOC. NOMINAL DEL CODEC $V_c = \frac{8L}{T}$

G711	64 Kbps
G726-36	32 Kbps
G729	8 Kbps
G721.1 MPMLQ	6,3
G721.1 ACELP	5,3

PDU = PROTOCOL DATA UNIT

EL CODEC { ENTREGA / RECIBE } LOS DATAGRAMAS ó PAYLOADS { AL / DEL } STACK DE PROTOCOLOS



L = 120, 160, 240
T = 20, 30, msg

PDU = PROTOCOL DATA UNIT

Seguiremos estudiando los CODEC utilizados en telefonía IP en el punto 6 de estos apuntes, después que hayamos analizado el protocolo Real Time transport Protocol (RTP) para la fase conversación.

Una vez que se hayan estudiado los protocolos utilizados en telefonía IP, se estará en condiciones de comprender mejor los principios de funcionamiento, las principales especificaciones y el ancho de banda requerido en la red de datos, por los CODEC. Estos aspectos se tratan en el punto 6.

3 Modelos OSI y TCP/IP

3.1 Introducción

3.2 Modelo OSI

3.2.1 Funciones y protocolos en el Modelo OSI

3.2.2 Capas en el Modelo OSI

3.2.3 Unidades de datos en las diferentes capas OSI

3.3 Modelo TCP/IP

3.3.1 Funciones y protocolos en el Modelo TCP/IP

3.3.2 Capas en Modelo TCP/IP

3.3.3 Unidades de datos en las diferentes capas TCP/IP

3.3.4 Diferencias y semejanzas de TCP/IP con OSI

3.3.5 Protocolos de capa de transporte: TCP, UDP, SCP

3.3.6 Protocolo de capa de red en TCP/IP: Protocolo IP

3.3.6.1 Introducción

3.3.6.2 Estudio del encabezamiento en los paquetes IP

3.1 Introducción

Teniendo en cuenta que la telefonía IP se basa en la transmisión de la voz paquetizada por redes de datos, en esta sección revisaremos conceptos fundamentales relacionados con la transmisión de datos y especialmente, con los protocolos TCP/IP.

- La familia de **protocolos TCP/IP** es la base de Internet y de muchas actuales redes corporativas

- Tanto el computador local como el distante contienen un grupo de programas que constituyen el software TCP/IP, al que se denomina **"stack de protocolos"**

- El “stack de protocolos” del computador local intercambia información con el “stack de protocolos” del computador distante y viceversa, con el fin de lograr la transferencia de datos entre ambos extremos

- La información que intercambian ambos stack de protocolos se refiere a:

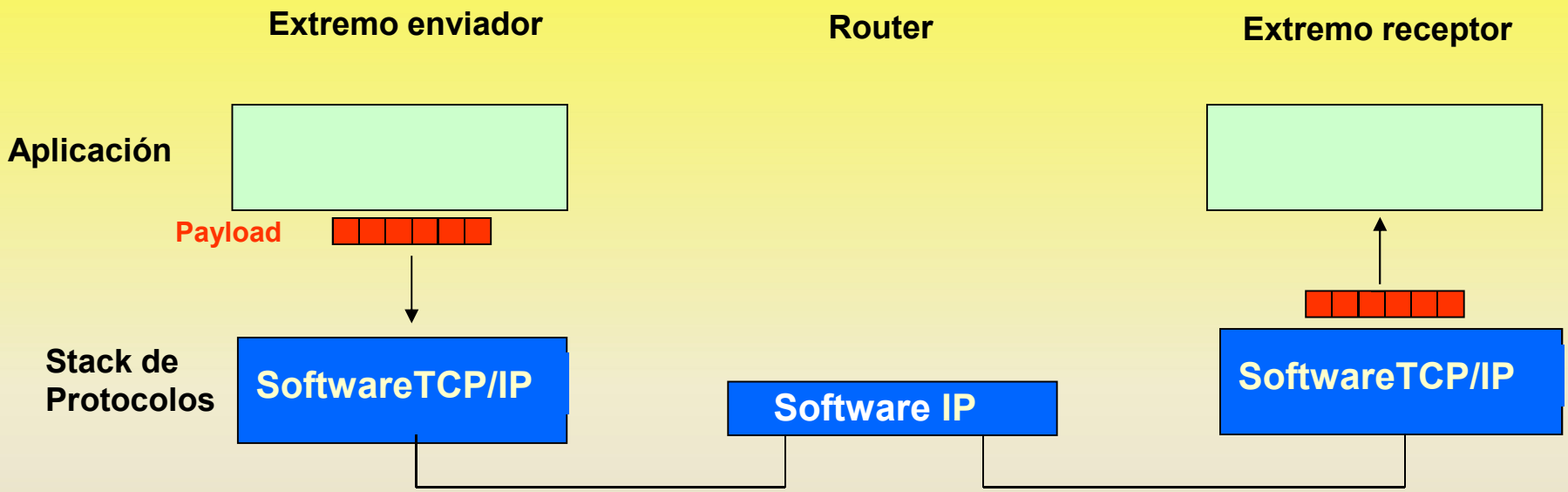
  - el tamaño de las porciones de datos (tamaño de payload)
  - la identificación asociada con cada payload
  - las acciones que se tomarán si una porción de datos se pierde o daña durante su viaje por la red

Payload: unidad de información que intercambian los extremos

- La Aplicación residente en el extremo enviador intercambia porciones de datos con la misma Aplicación residente en el extremo receptor. Estas porciones de datos, que llamaremos “payload”, corresponden a la “carga útil” que se transmite extremo a extremo. Para transmitirlos por la red, los payload se encapsulan en otros tipos de unidades de datos, que revisaremos más adelante.

- Estas porciones de datos son las unidades de información que intercambian los extremos. Puede que sea necesario fragmentarlos para ser transferidos a través de los diversos “segmentos” ó “saltos” que conforman la red.

- El Stack de Protocolos TCP/IP determina como serán transferidas las porciones de datos desde el programa de envío hasta el programa de recepción, a través de la red IP.



3.2 Modelo OSI

Modelo de Referencia para la Interconexión de Sistemas Abiertos (Open System Interconection)

3.2.1 Funciones y protocolos en el Modelo OSI

En el modelo OSI se distinguen el MEDIO FISICO y 7 CAPAS. La cantidad de 7 capas se decidió como un compromiso entre:

- la necesidad de que el número de capas sea el menor posible para que el modelo resulte simple y práctico.
- la necesidad de tener suficientes capas para que cada una reúna pocas funciones, evitando descripciones demasiado complejas
- la necesidad de seleccionar fronteras naturales para las funciones dentro de cada capa, para minimizar las interacciones entre capas

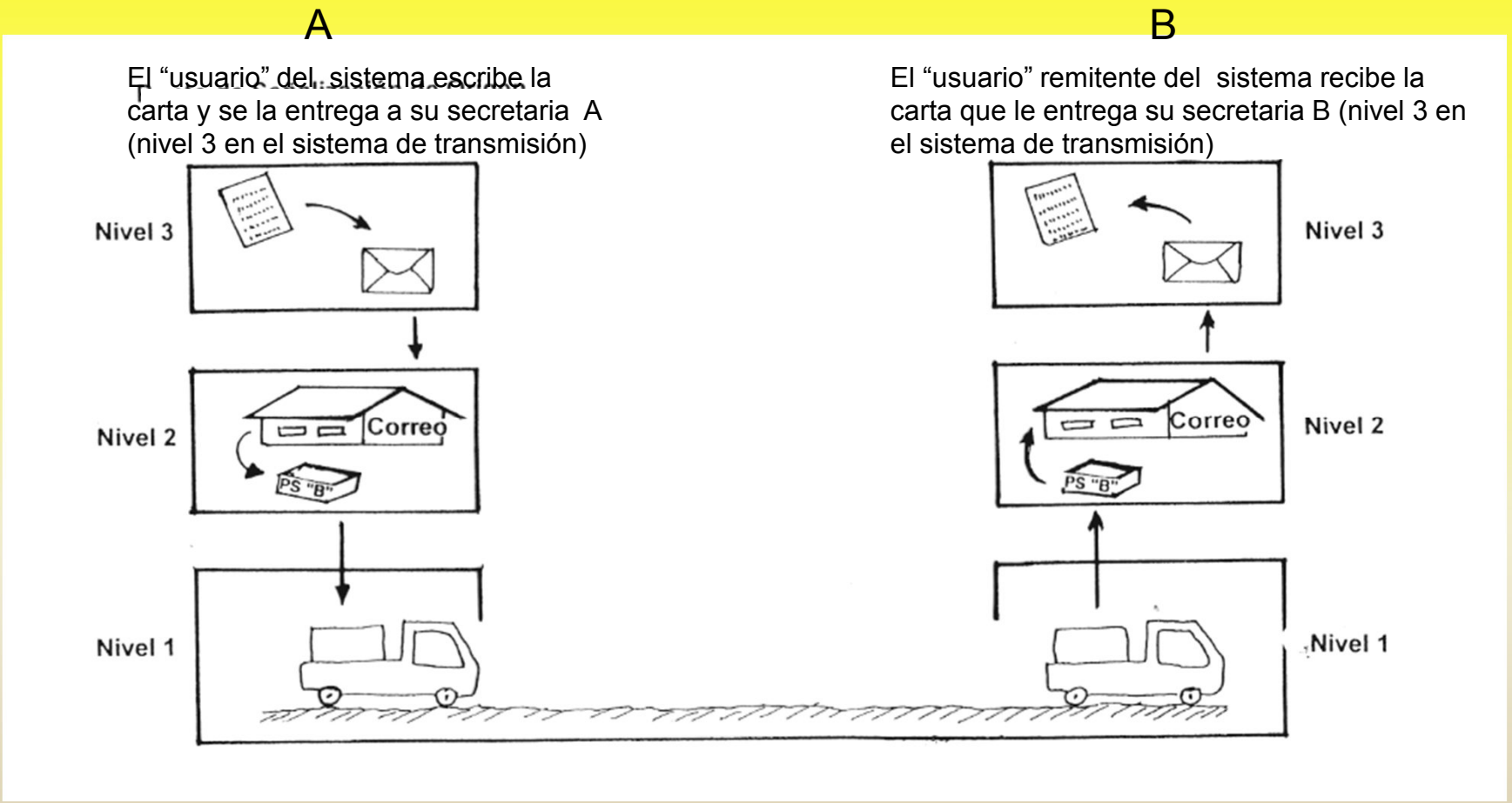
Los modelos de referencia sistematizan (con el objetivo de estandarizar) los procesos requeridos para la transmisión de datos entre computadores

Crean arquitecturas que tienen como objetivo proporcionar un esqueleto alrededor del cual se pueden diseñar protocolos específicos que permitan a diferentes usuarios, comunicarse "abiertamente".

Los Modelos de Referencia identifican las funciones que se requieren realizar para una comunicación de datos y las clasifican, asignándolas a capas o niveles.

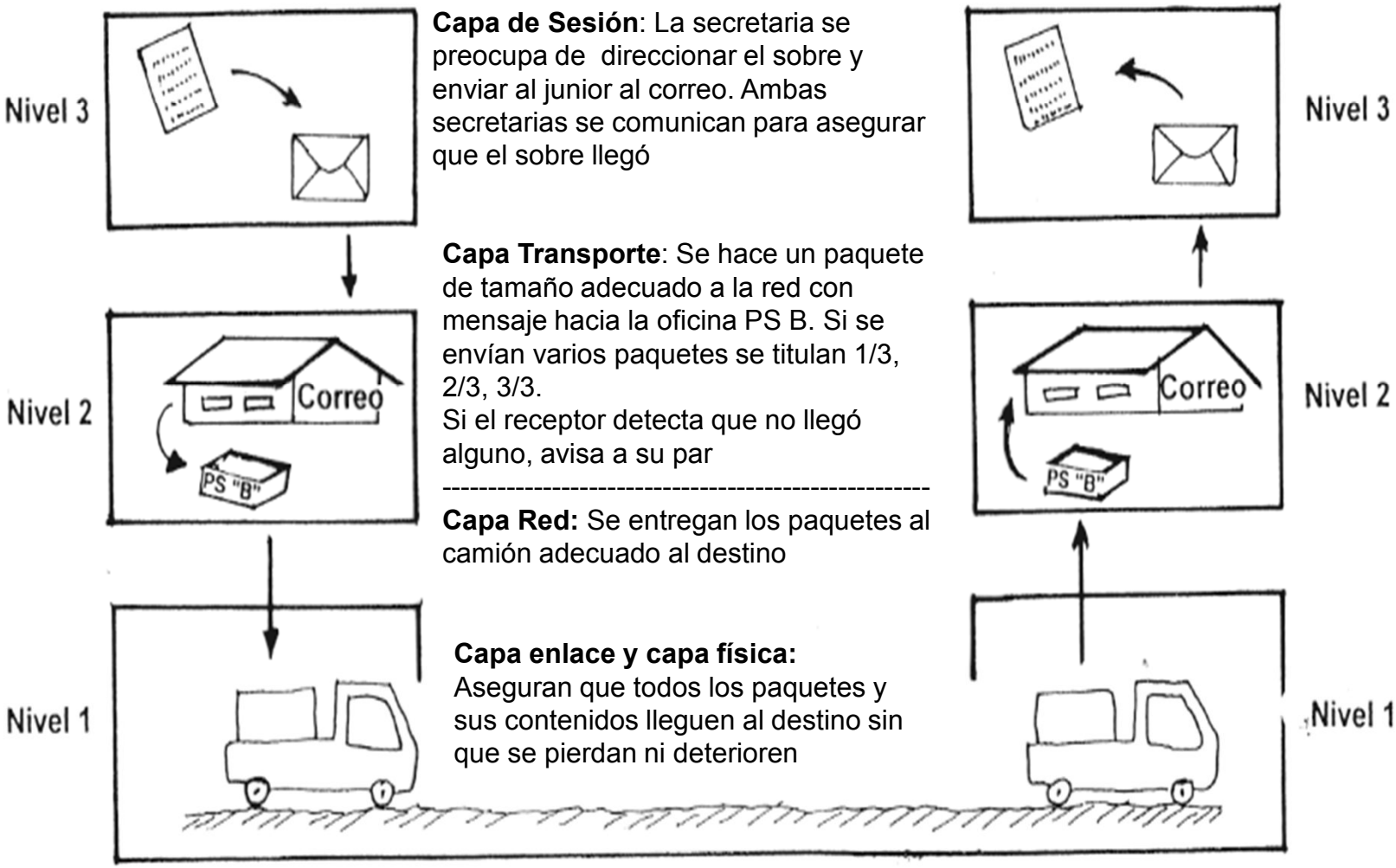
El nivel más alto, que corresponde a la "aplicación", es el que efectivamente hace uso del sistema, estando todos los niveles inferiores, a su servicio.

Un ejemplo simple: Modelo de 3 capas o niveles para envío y recepción de carta desde oficina A hacia oficina B



Algunas funciones de capas

Capa Aplicación: El usuario cuida la semántica (*) del mensaje.
Capa Presentación: El usuario cuida la sintaxis del mensaje
El usuario genera payloads



Capa de Sesión: La secretaria se preocupa de direccionar el sobre y enviar al junior al correo. Ambas secretarias se comunican para asegurar que el sobre llegó

Capa Transporte: Se hace un paquete de tamaño adecuado a la red con mensaje hacia la oficina PS B. Si se envían varios paquetes se titulan 1/3, 2/3, 3/3.
Si el receptor detecta que no llegó alguno, avisa a su par

Capa Red: Se entregan los paquetes al camión adecuado al destino

Capa enlace y capa física:
Aseguran que todos los paquetes y sus contenidos lleguen al destino sin que se pierdan ni deterioren

(*) Semántica = Significado de una expresión sintácticamente bien construida

El modelo OSI define claramente los siguientes conceptos:

Servicio: Cada capa proporciona servicios a la capa inmediatamente superior. Servicio es el valor que la capa agrega o el aporte que la capa hace para transferir la información.

Interfaz: La interfaz de una capa especifica los resultados que la capa entrega y los parámetros que espera como entradas para realizar el servicio requerido

Protocolo: Cada protocolo es una forma para realizar el diálogo conducente a realizar un servicio, entre una capa enviadora y la misma capa en el lado receptor

Considerando los servicios que cada capa entrega a la inmediatamente superior, éstas cumples funciones de red o funciones de usuario

FUNCIONES de USUARIO FINAL

- Las 4 capas superiores del modelo OSI realizan FUNCIONES de USUARIO FINAL.
- Las funciones de usuario final, se realizan por completo en los dispositivos del usuario.
- Los protocolos que utilizan las cuatro capas superiores se clasifican como protocolos de alto nivel.
- Los protocolos de capas 7, 6, 5 y 4 dialogan directamente entre los computadores de origen y destino, usando para el diálogo los encabezamientos de la respectiva capa.

FUNCIONES de RED

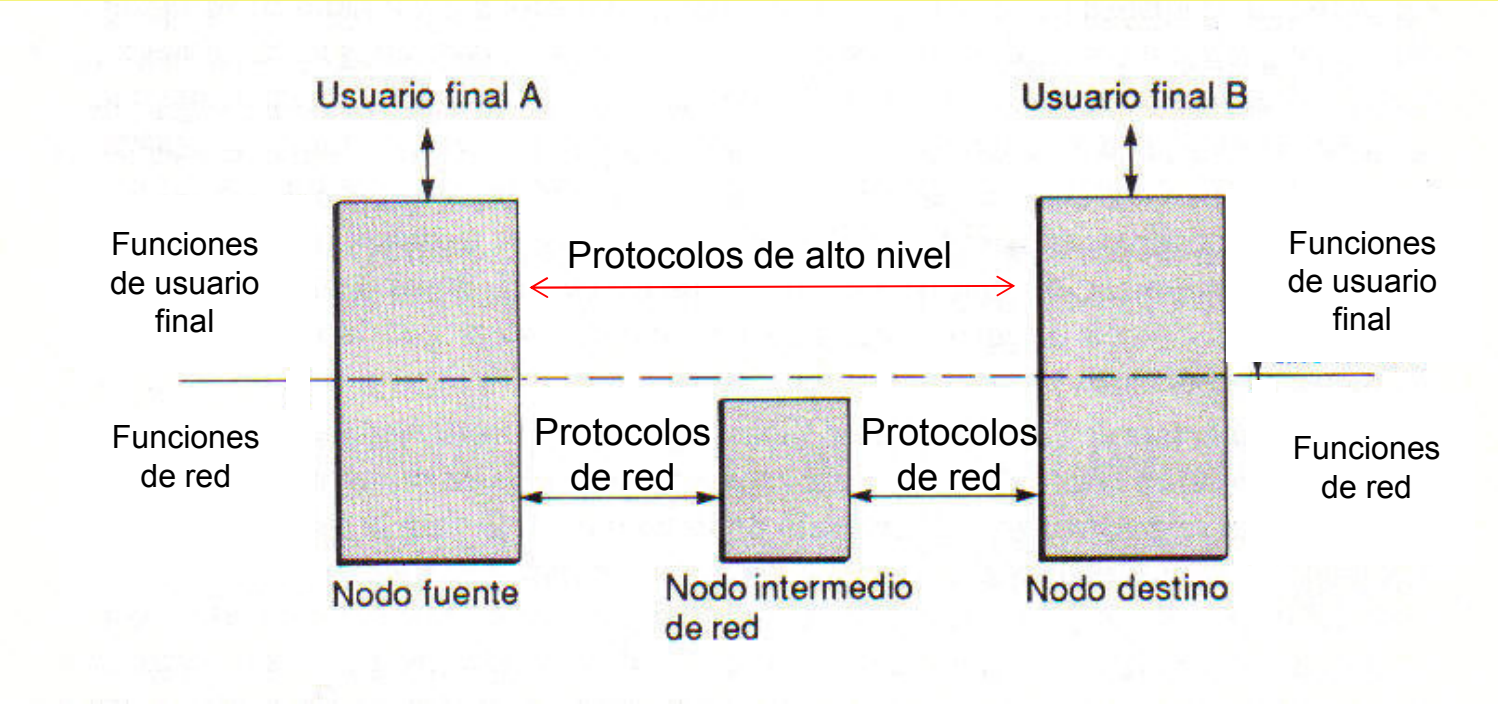
- Las 3 capas inferiores realizan FUNCIONES de RED.
- Las funciones de red muchas veces se realizan en routers de la red, a cargo de empresas externas sobre las que el usuario no tiene control.
- Los protocolos que estas capas utilizan se clasifican como protocolos de red.
- La capa más inferior corresponde al MEDIO FISICO.
- Los protocolos de capas 3, 2 y 1 dialogan siempre entre cada máquina y sus vecinas inmediatas, usando para el diálogo los encabezamientos de la respectiva capa.

PROTOCOLOS DE ALTO NIVEL

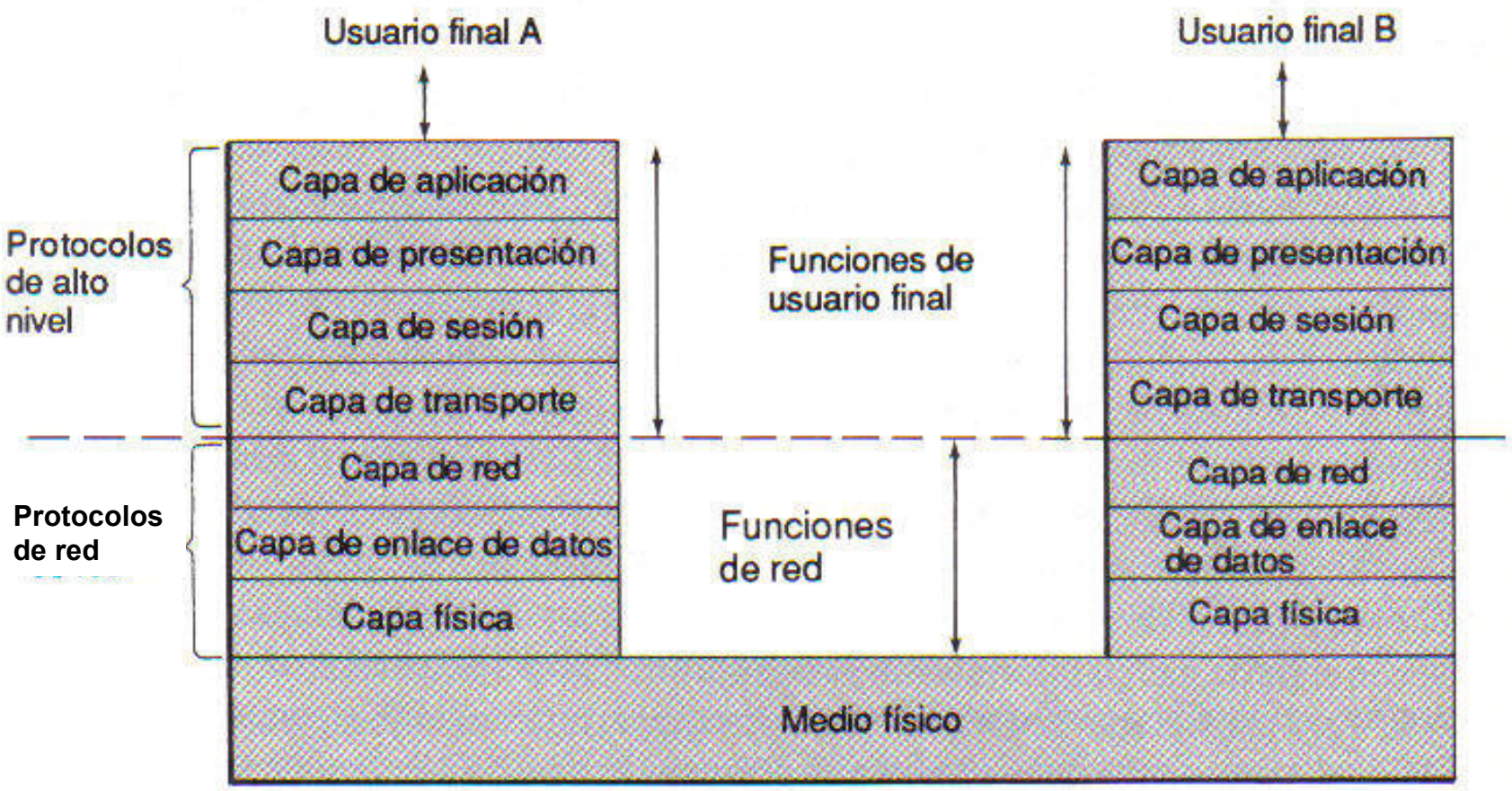
Los PROTOCOLOS DE ALTO NIVEL aseguran que los datos que se entregan al destino están en el formato adecuado y son reconocibles

PROTOCOLOS DE RED

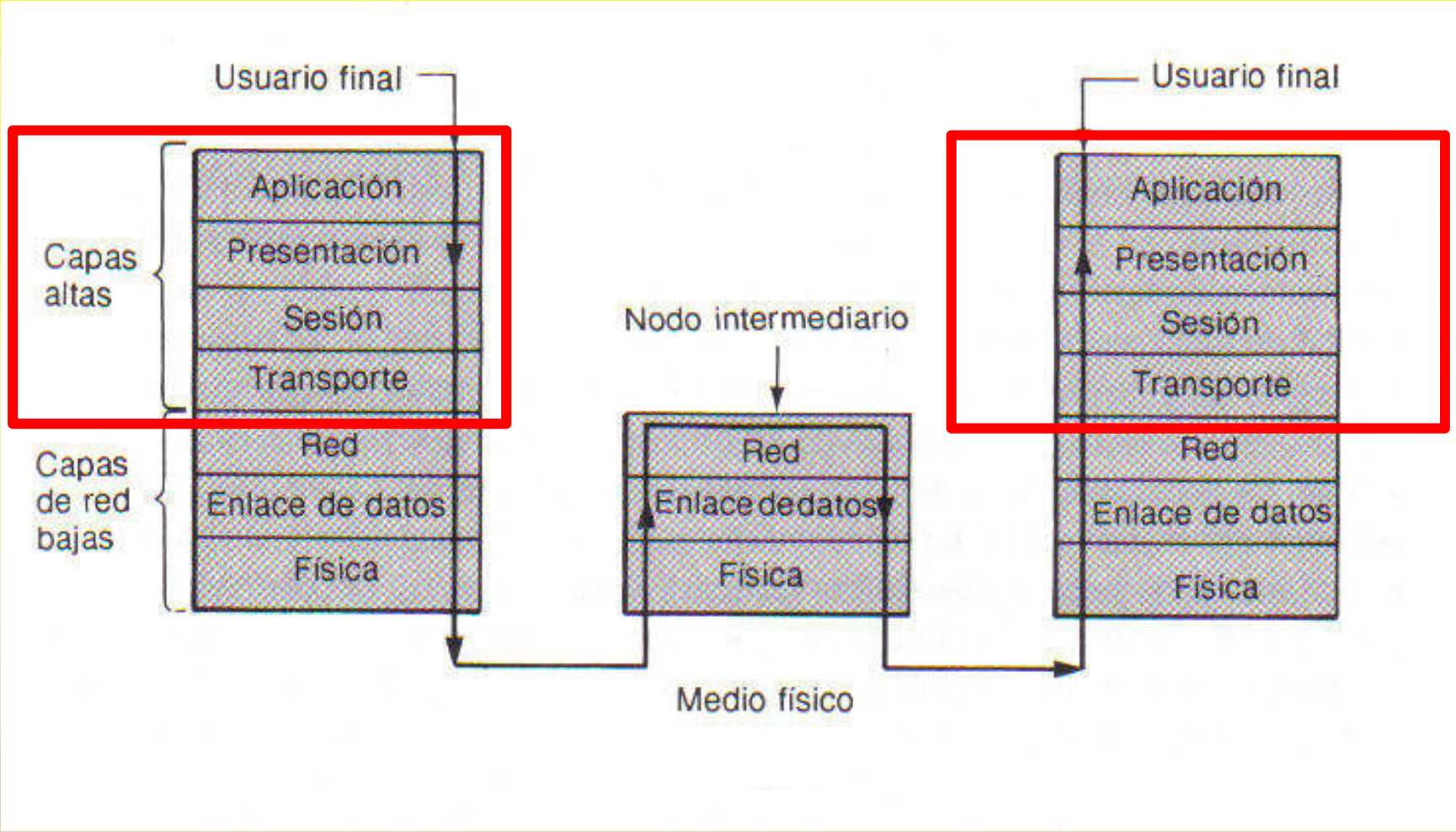
Los PROTOCOLOS DE RED aseguran que los datos del emisor son dirigidos y llegan al destino correcta y ordenadamente



3.2.2 Capas en el Modelo OSI



a) CAPAS OSI QUE REALIZAN FUNCIONES DE USUARIO FINAL (protocolos de alto nivel)



Cada capa realiza las funciones que tiene asignadas tanto en el extremo enviador, como en el extremo receptor

CAPA de APLICACIÓN (capa 7)

La CAPA de APLICACIÓN mediante sus protocolos del nivel de aplicación, proporciona la **semántica** o interpretación adecuada a los datos intercambiados (1).

NOTA:

(1) La semántica se preocupa del significado de una expresión sintácticamente bien construida

CAPA de PRESENTACION (capa 6)

La CAPA de PRESENTACION se encarga de la **sintaxis** (1) de las unidades de datos que se intercambian entre los usuarios finales.

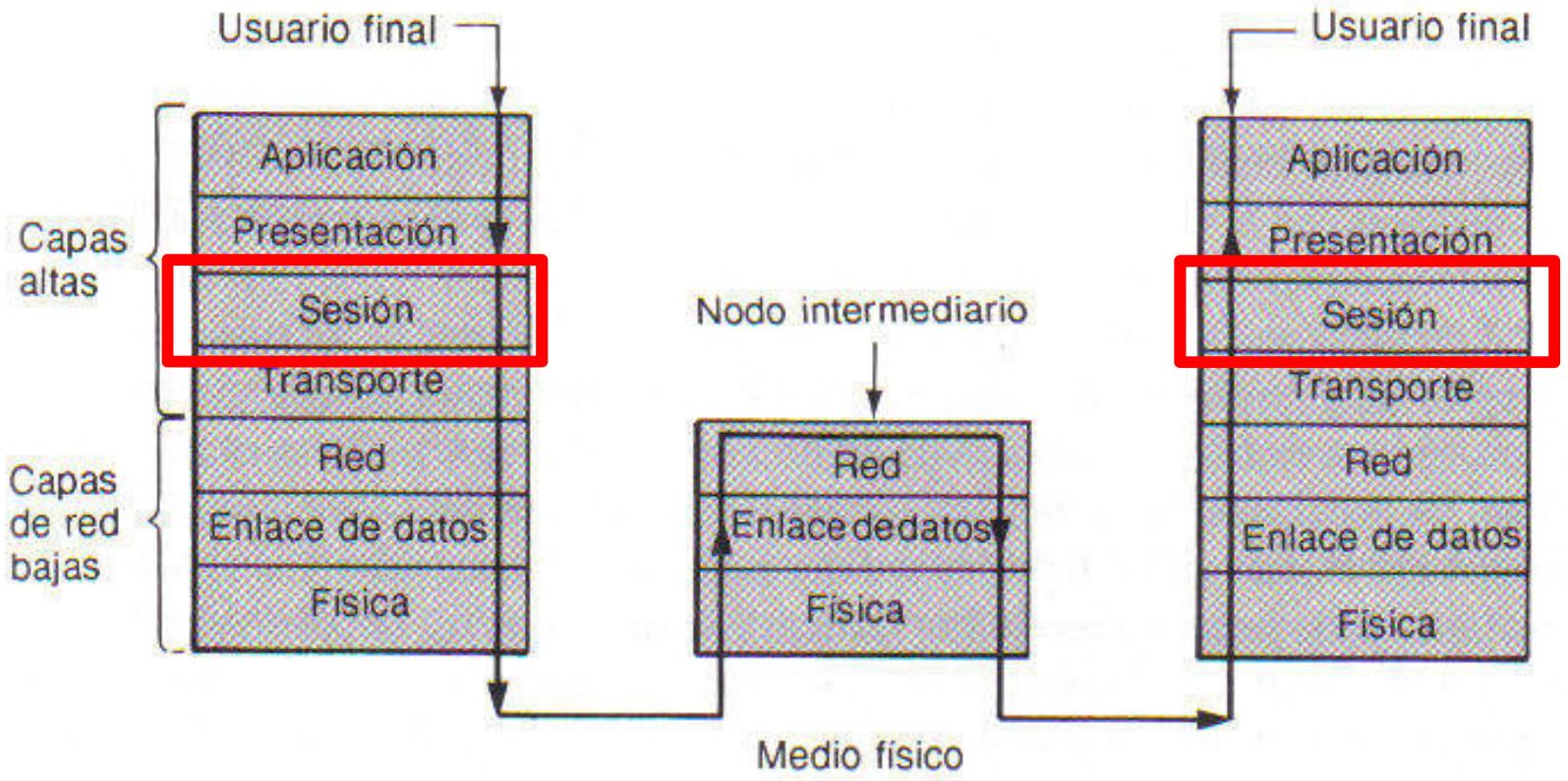
Esta capa proporciona:

Códigos para convertir los caracteres:	pattern de bits para representar cada carácter
Algoritmos de encriptación:	forma en que se encripta la información que se envía en los payload
Compresión de datos:	forma en que se comprime la información que se envía en los payload

Permite que computadores que usan diferentes formas para representar los datos, se puedan comunicar entre ellos, cuando ambos computadores entregan y reciben los datos según los protocolos acordados para capa 6

NOTA:

(1) La sintaxis establece reglas para combinar constituyentes (palabras) y formar unidades superiores (oraciones)


Usuario final
Usuario final
Capas altas
Capas de red bajas
Aplicación
Presentación
Sesión
Transporte
Red
Enlace de datos
Física
Nodo intermediario
Red
Enlace de datos
Física
Aplicación
Presentación
Sesión
Transporte
Red
Enlace de datos
Física
Medio físico

CAPA de SESION (capa 5)

Sesión = comunicación entre usuarios durante la que se transmiten los mensajes

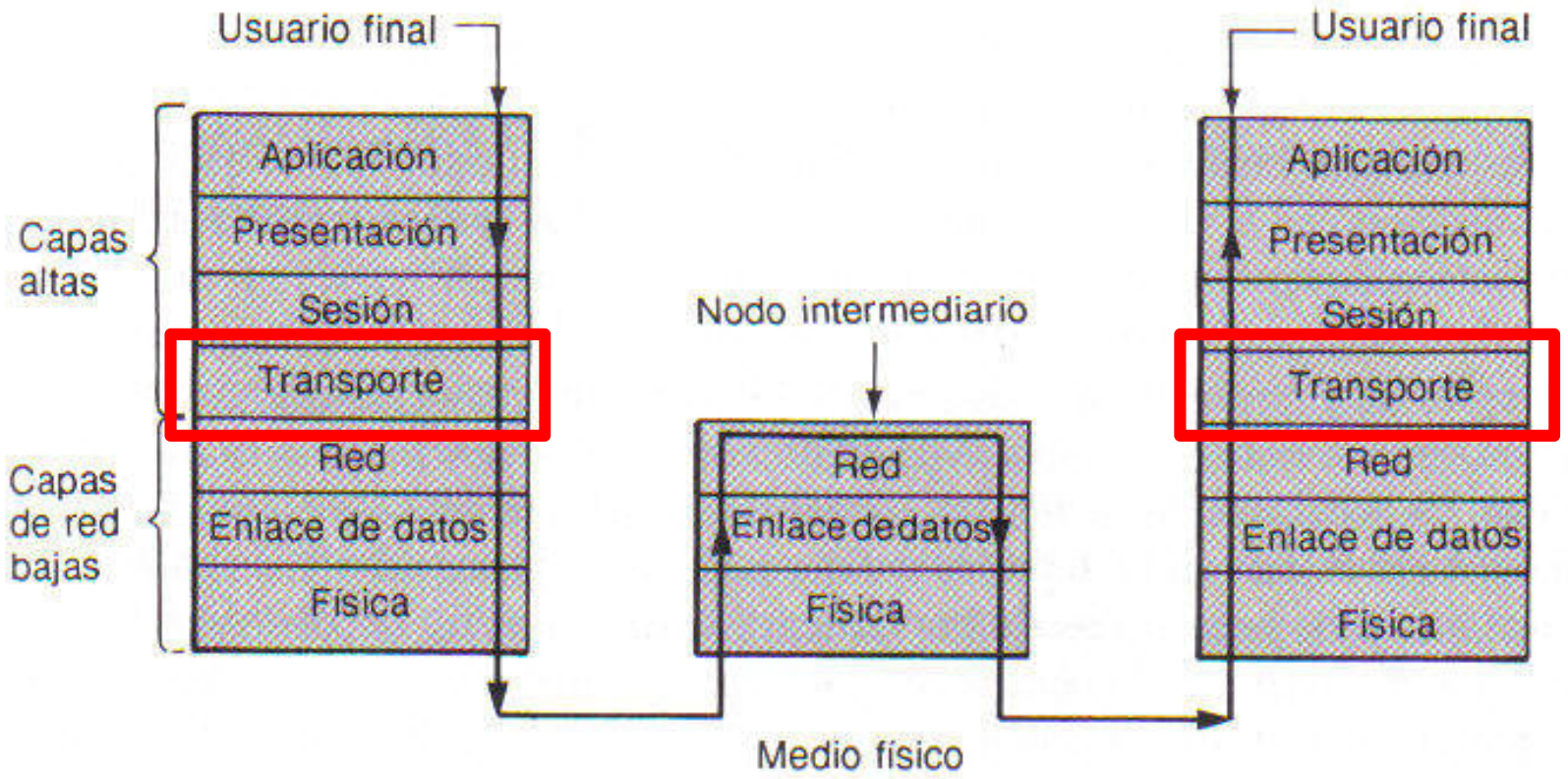
La capa de sesión recibe de la capa de transporte el servicio de transporte virtual de mensajes extremo-extremo

La CAPA de SESION realiza las tareas de **establecimiento y desconexión de sesión**. Cuando es necesario, esta capa también administra la sesión a fin de asegurar un intercambio ordenado de los datos.
La capa ofrece servicio de control de diálogo (determinando a quién le toca transmitir), servicio de sincronización (en caso que la sesión se interrumpa, para restablecerla en el punto en que se encontraba antes de la interrupción) y servicio de token (para evitar que las dos partes realicen una misma operación crítica a la vez)

También son tareas típicas de la CAPA DE SESIÓN, la administración de asistencia a sesiones (directorio de asistencia), de derechos de acceso, de facturación….

Se ha demostrado que no es práctico estandarizar la capa **Presentación** ni la capa **Sesión**, ya que la comunicación entre Aplicación y capa de Transporte está siempre en el sistema operativo, no requiriéndose interfaces estandarizados.

Por este motivo, como veremos más adelante, el modelo TCP/IP omite estas dos capas.


Usuario final
Usuario final
Capas altas
Capas de red bajas
Aplicación
Presentación
Sesión
Transporte
Red
Enlace de datos
Física
Nodo intermediario
Red
Enlace de datos
Física
Aplicación
Presentación
Sesión
Transporte
Red
Enlace de datos
Física
Medio físico

CAPA de TRANSPORTE (capa 4)

Las funciones de la capa de transporte son:

- Dividir y reensamblar los mensajes en paquetes de tamaño adecuado a la capa de red
- Permitir sesiones múltiples con un mismo nodo fuente/destino
- Resecuenciar los paquetes en el destino
- Recuperación de errores residuales y fallas
- Proveer control de flujo extremo-extremo

CAPA de TRANSPORTE (capa 4)

En el modelo OSI la CAPA de TRANSPORTE asegura el intercambio eficiente y confiable de los datos entre los usuarios finales, independientemente de la red o redes físicas utilizadas para dicho intercambio.

En el modelo OSI la capa de transporte proporciona siempre **servicio de transporte orientado a la conexión.** Es decir la capa de transporte se preocupa de asegurar a las capas superiores que los mensajes se transmiten OK extremo-extremo. La capa de transporte proporciona un servicio de mensajes virtual extremo-extremo a las capas superiores.

La forma de hacerlo es: Cuando llega OK el segmento de datos al destino, la capa de transporte receptora envía hacia la parte transmisora un segmento de datos (el que puede o no encapsular payload) que contiene el nº de secuencia del segmento siguiente al que recibió OK (el que ahora está esperando recibir).

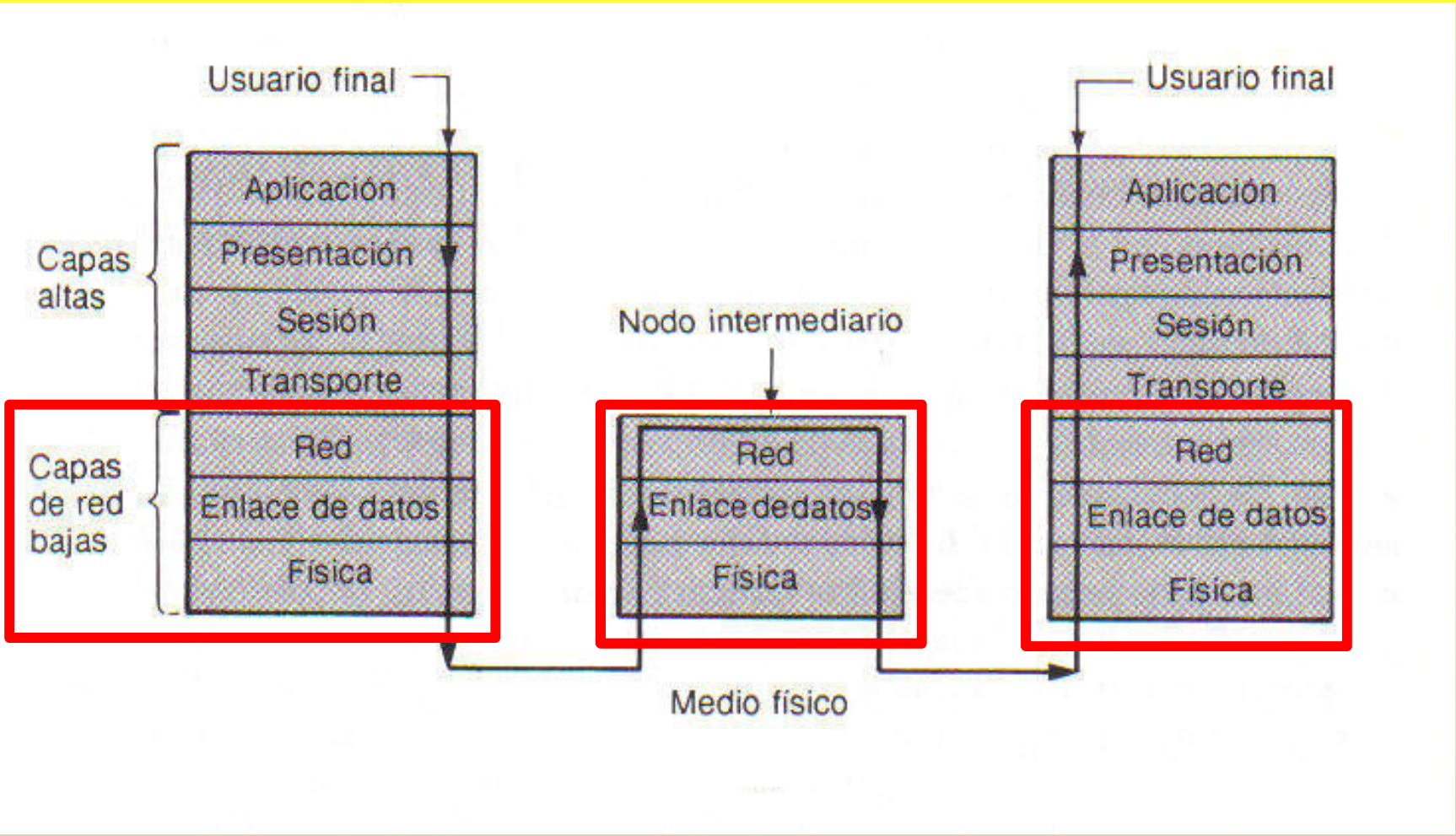
Se requiere este servicio en la capa de transporte porque ella hace funciones de usuario final, lo que significa que los procesos de transporte se realizan por completo en los dispositivos de usuario, contrariamente a lo que ocurre con la capa de red, en que los procesos se realizan muchas veces también en routers de la red, a cargo de empresas externas sobre las que el usuario no tiene control.

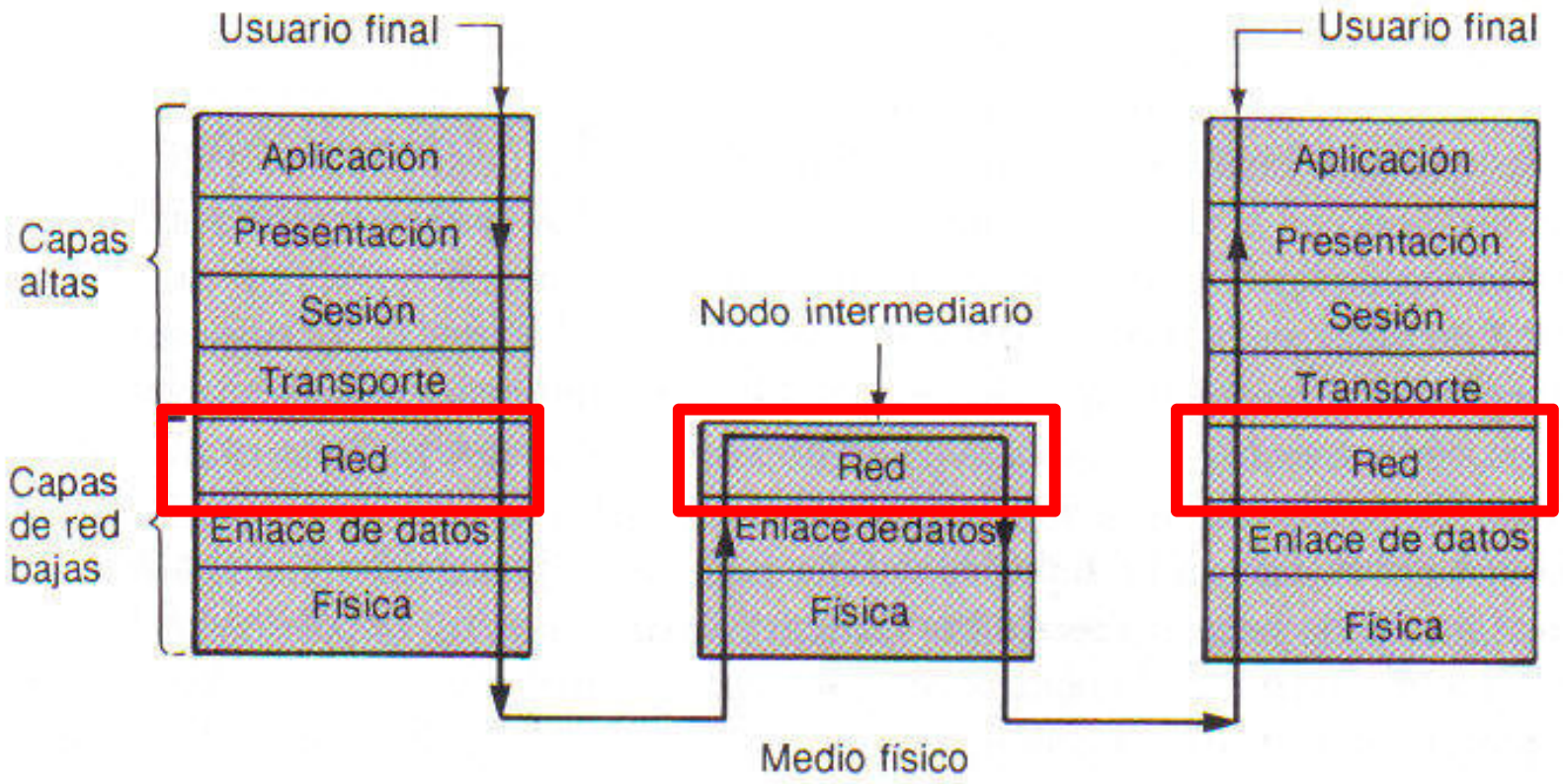
Si durante una sesión de transmisión de datos la capa de transporte orientada a la conexión es informada por la capa de red que su conexión de red se interrumpió, la capa de transporte establece una nueva conexión con la capa de transporte remota. Usando la nueva conexión de red, la capa de transporte pide a su igual remota indicar el último dato recibido correctamente a fin de reiniciar desde allí la transmisión.

Otro servicio que entrega la capa de transporte es control de flujo:

Debido a que distintos sistemas finales pueden transmitir unidades de datos a diferentes velocidades, un sistema rápido podría saturar a otros más lentos, a menos que exista un control de estos flujos. Esta función que asegura la recepción ordenada de las unidades de datos, la realiza la capa de transporte.

b) CAPAS OSI QUE REALIZAN FUNCIONES DE RED




Usuario final
Usuario final
Aplicación
Presentación
Sesión
Transporte
Red
Enlace de datos
Física
Capas altas
Capas de red bajas
Nodo intermediario
Red
Enlace de datos
Física
Aplicación
Presentación
Sesión
Transporte
Red
Enlace de datos
Física
Medio físico

Las capas 3 y 2 proveen un enlace de comunicaciones libre de errores entre dos nodos de la red

Capa de red

- El módulo capa de red acepta paquetes provenientes de la capa de transporte y paquetes en tránsito provenientes de la capa enlace de datos
- Esta capa en el origen enruta cada paquete al enlace de datos saliente. En el destino enruta los paquetes a la capa de transporte
- La capa de red agrega su propios encabezamientos a los paquetes recibidos desde la capa de transporte. Estos encabezamientos proporcionan la información necesaria para el enrutamiento (por ej. dirección de destino)

Todo nodo de la red contiene un módulo capa de red, un módulo enlace de datos y un módulo correspondiente a la capa física.

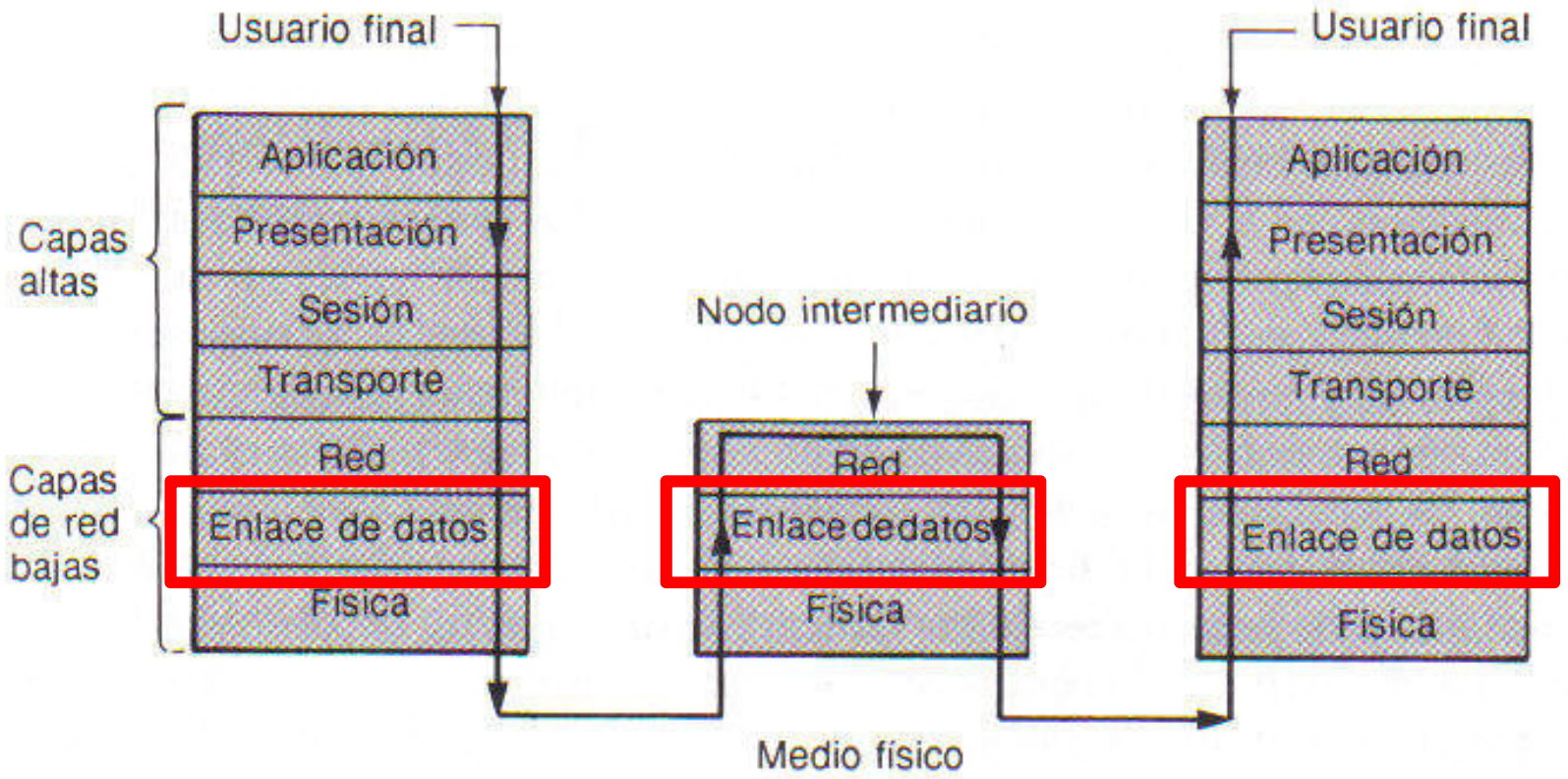
CAPA de RED (capa 3)

Tiene por función dirigir los datos desde el nodo fuente al nodo destino a través de la red, o de varias redes, cuando es necesario. De esta forma proporciona a la capa de transporte el servicio de enrutar paquetes entre origen y destino. La capa de red puede dar el servicio de enrutamiento de dos formas:

- **Servicio de red orientado a la conexión:** se establecen circuitos virtuales; la decisión de enrutamiento se toma al establecer el circuito virtual
- **Servicio de red no-orientado a la conexión**: la información se transmite en modo datagramas. La decisión de enrutamiento se toma al analizar el encabezamiento de cada paquete. La capa de red proporciona un tubo virtual extremo-extremo a la capa de transporte.

La capa de red también proporciona servicios de control de flujo o control de congestión, para evitar que los recursos de red (enlaces de transmisión y buffers de almacenamiento temporal en los nodos) se saturen provocando situaciones de bloqueo mutuo.

Como veremos más adelante, en el modelo TCP/IP la capa de red (IP) proporciona solamente el servicio no-orientado a la conexión.


Usuario final
Usuario final
Capas altas
Capas de red bajas
Aplicación
Presentación
Sesión
Transporte
Red
Enlace de datos
Física
Nodo intermediario
Red
Enlace de datos
Física
Aplicación
Presentación
Sesión
Transporte
Red
Enlace de datos
Física
Medio físico

CAPA ENLACE DE DATOS (capa 2)

Los Protocolos Enlace de Datos aseguran que los bloques de datos (tramas) se transfieran a través del enlace en forma secuencial y sin errores (en forma confiable). Al respecto en esta capa se identifican las siguientes funciones:

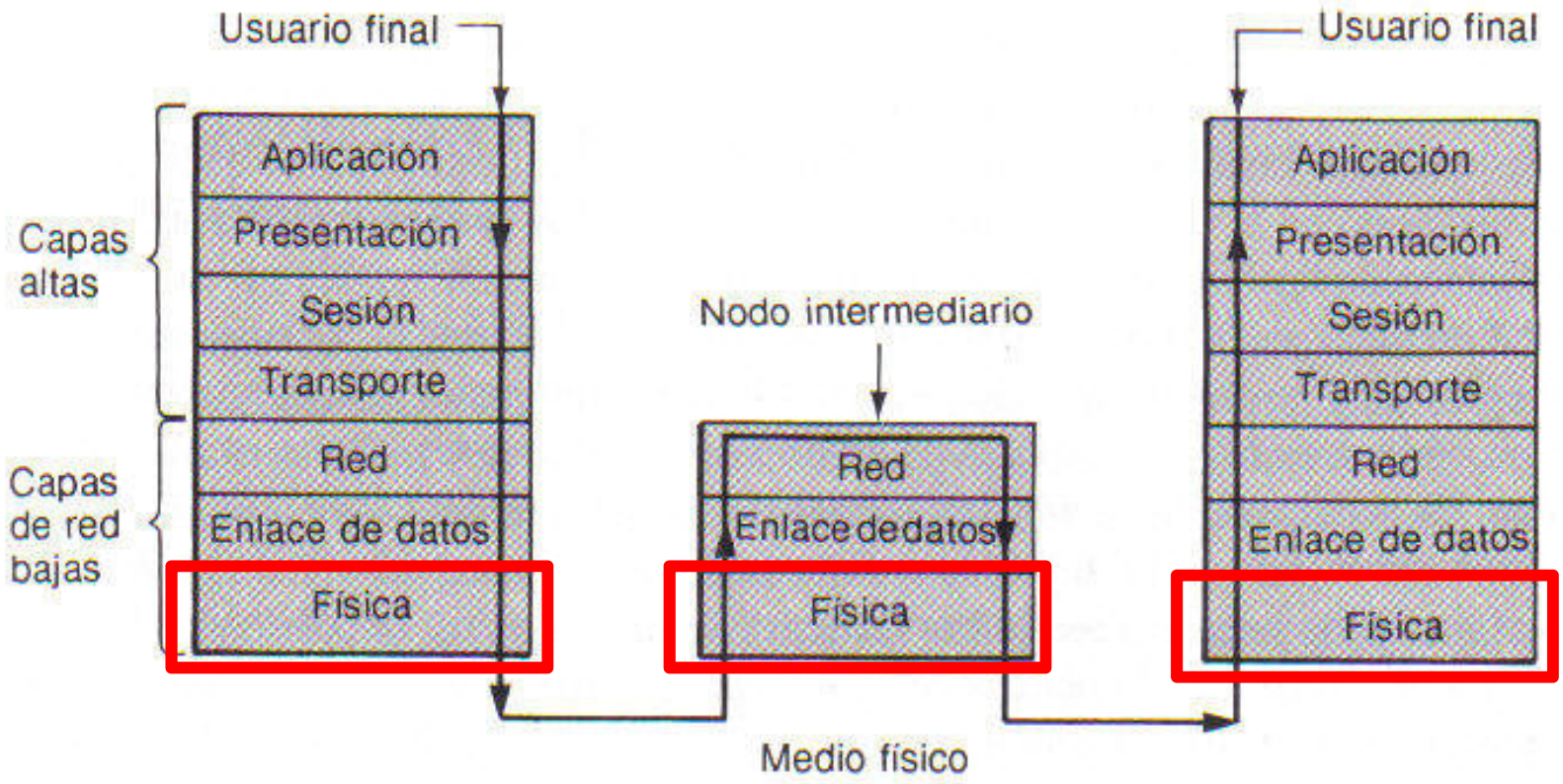
Detección de errores: Consiste en determinar cuales PDU contienen errores

Corrección de errores: La corrección de errores se hace pidiendo la retransmisión de la trama en que se detectó error. (Automatic Repeat Request [ARQ])

Framing: Consiste en determinar los bit de inicio y término de la trama. El primer bit de una trama está sincronizado para funciones de reconocimiento de fin de trama así como funciones de detección y corrección de errores.

Se define la subcapa de “control de acceso al medio” la cual asigna el direccionamiento físico de destino. Esta dirección, no modificable y única para cada dispositivo de hardware, permite a los host en el lado receptor identificar las tramas dirigidas a ellos.

En esta capa y en las superiores hay que preocuparse de controlar los flujos para evitar que un transmisor rápido sature a receptores lentos. Esto se hace informando al transmisor el espacio libre en el buffer receptor.


Usuario final
Aplicación
Presentación
Sesión
Transporte
Red
Enlace de datos
Física
Capas altas
Capas de red bajas
Nodo intermediario
Red
Enlace de datos
Física
Usuario final
Aplicación
Presentación
Sesión
Transporte
Red
Enlace de datos
Física
Medio físico

CAPA FISICA (capa 1)

Tiene por función asegurar que cada bit que entra al MEDIO FISICO DE TRANSMISION, llegue a su destino.

La capa garantiza que si se envió un 1, en el lado receptor se reciba un 1 y no un 0

Especifica parámetros y características técnicas como las siguientes:

- Niveles de tensión para representar un 1 y un 0
- Tiempo durante el que se transmite un bit
- Cantidad de pines y configuración de los conectores
- Transmisión en un solo sentido o en ambos a la vez
- Forma de iniciar y de finalizar el envío

En el medio físico ocurren:

Retardos de propagación:

Las señales viajan aproximadamente a la velocidad de la luz (C = $3x10^8$ metros/seg.):

Satélite GEO (d = 40.000 Km.) ➔ 125 miliseg. retardo
Satélite LEO (d = 1.000 Km.) ➔ 3,3 miliseg. retardo
Cable Ethernet (d = 1 Km.) ➔ 0,3 miliseg. retardo

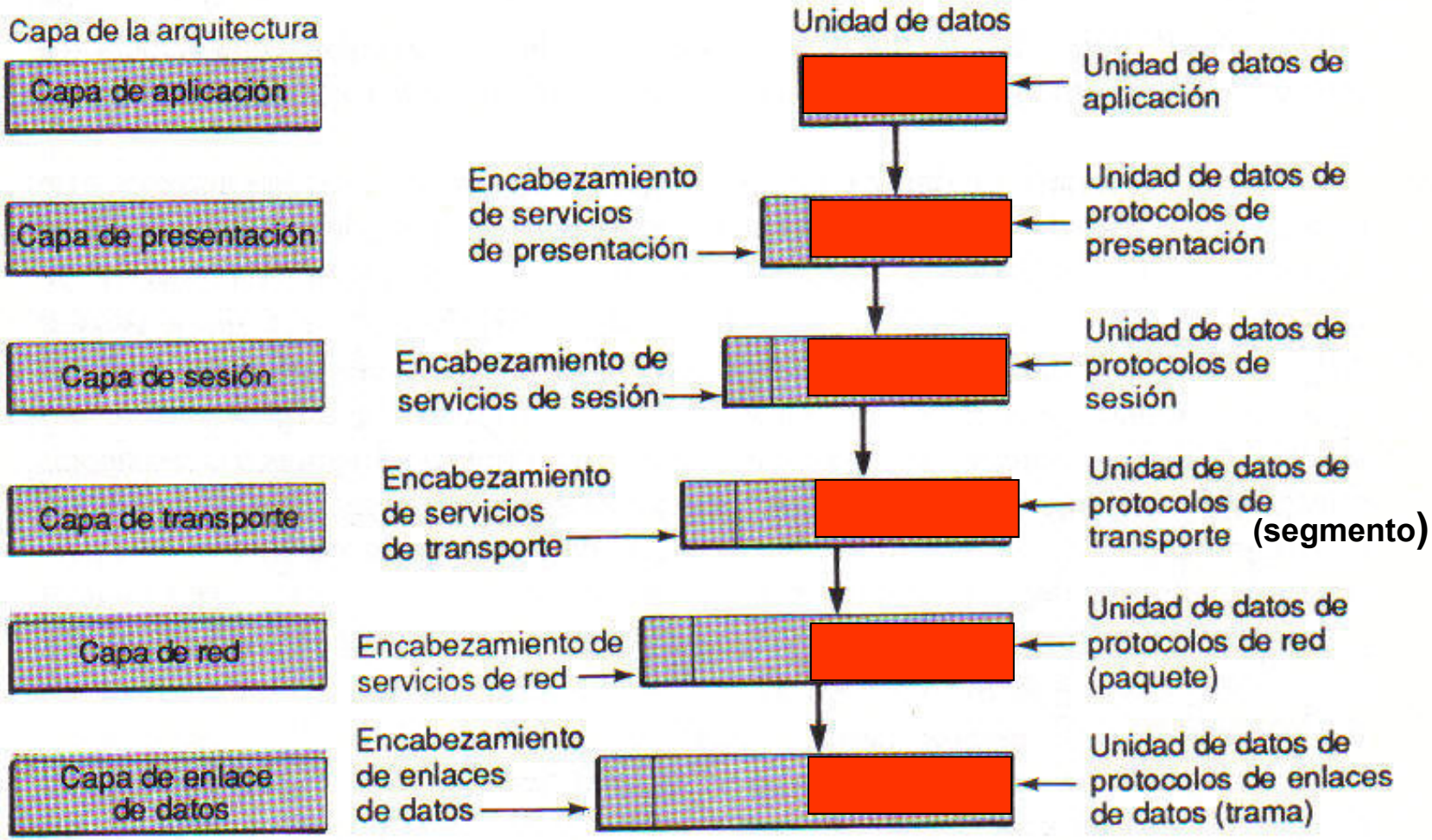
LEO = Low Earth Orbit

Errores de transmisión:

Cada bit que se transmite tiene probabilidad de llegar erróneo:
Porque la atenuación del medio físico hace que la señal pierda potencia
Porque el ruido existente en el medio físico provoca interferencias

En la práctica los errores se concentran en “ráfagas de errores”

3.2.3 Unidades de datos en las diferentes capas OSI



En el modelo OSI a estas unidades de datos intercambiadas par a par entre capas, se les denomina Protocol Data Unit (PDU).

Como hemos visto, las PDU pueden contener información de control, información de direccionamiento o datos.

La PDU en capa 1 es el Bit
La PDU en capa 2 es la Trama
La PDU en capa 3 es el Paquete
La PDU en capa 4 es el Segmento
La PDU en las capas 5 y superiores es conocida como Datos

Los modelos de referencia sistematizan (con el objetivo de estandarizar) los procesos requeridos para la transmisión de datos entre computadores

Crean arquitecturas que tienen como objetivo proporcionar un esqueleto alrededor del cual se pueden diseñar protocolos específicos que permitan a diferentes usuarios, comunicarse "abiertamente".

Los Modelos de Referencia identifican las funciones que se requieren realizar para una comunicación de datos y las clasifican, asignándolas a capas o niveles.

El nivel más alto, que corresponde a la "aplicación", es el que efectivamente hace uso del sistema, estando todos los niveles inferiores, a su servicio.

El nivel superior "encarga" tareas al nivel inmediatamente inferior.

El nivel inferior "sirve" al nivel inmediatamente superior.

En una comunicación entre dos Puntos A y B, cada nivel de A dialoga con su par en B.

El diálogo es par a par.

3.3 Modelo TCP/IP

TCP/IP no sigue estrictamente el modelo OSI.

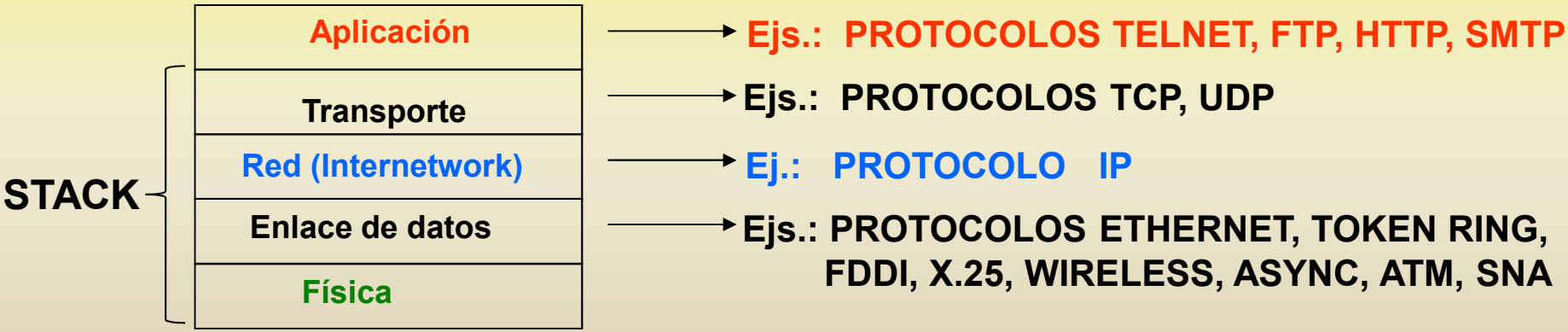
Es una implementación de facto, en que se distingue menor cantidad de capas que las definidas por OSI

No existe pleno acuerdo para la definición de las capas

3.3.1 Funciones y protocolos en Modelo TCP/IP

Funciones de usuario final: Aplicación
Transporte

Funciones de red: Red (Internetwork)
Enlace de datos
Física



3.3.2 Capas en el Modelo TCP/IP

CAPA APLICACIÓN

La capa proporciona funcionalidades correspondientes a procesos de usuario que cooperan con otros procesos de usuario, en el mismo computador o en otro computador.

Algunos ejemplos:

- TELNET, protocolo diseñado para la conexión de terminales remotos
- FILE TRANSFER PROTOCOL (FTP), protocolo para transmitir archivos
- SIMPLE MAIL TRANSFER (SMTP), protocolo para transmitir correos
- HIPER TEXT TRANSFER PROTOCOL (HTTP), protocolo para envío de mensajes tipo requerimiento/respuesta
- **PROTOCOLOS TELEFONIA IP ….**

CAPA TRANSPORTE

La capa proporciona las funcionalidades para la transferencia de datos entre ambos extremos.

El objetivo es asegurar el intercambio eficiente y confiable de los datos entre los usuarios finales, independientemente de la red o redes físicas utilizadas para dicho intercambio.

Los principales protocolos de transporte en TCP/IP:

TRANSMISSION CONTROL PROTOCOL (TCP), protocolo orientado a la conexión, con control de flujo y de errores

USER DATAGRAM PROTOCOL (UDP), protocolo no orientado a la conexión

CAPA RED (INTERNETWORK)

La capa proporciona funcionalidades de red, preocupándose del encaminamiento de los paquetes por la red IP.

INTERNET PROTOCOL (IP) es un protocolo no orientado a la conexión, que supone que las capas inferiores son confiables por lo que no provee control de flujo. Esta funcionalidad debe ser proporcionada en las capas superiores (por TCP o por la Aplicación, en caso de uso de UDP)

Los routers deciden hacia donde dirigir cada paquete, es decir deciden el próximo salto. En cada router se va decidiendo la forma de seguir hacia delante

CAPA ENLACE DE DATOS

Esta capa, también llamada capa de enlace o capa interface de red, constituye la interface con el hardware físico de la red.

Ejemplos:

IEEE 802.2, X.25, ATM, FDDI, Ethernet, PRN (Packet Radio Network)

CAPA FÍSICA

Transmite los bits en forma de impulsos eléctricos, ondas electromagnéticas o de luz

3.3.3. UNIDADES DE DATOS EN LAS DIFERENTES CAPAS DEL MODELO TCP/IP

Unidades de datos en la capa Aplicación:

La capa Aplicación entrega la información que se debe transmitir por la red, organizada en porciones de datos llamadas **PAYLOAD** al stack de protocolos, el cual proporciona el servicio de transmisión de datos

Unidades de datos en la capa Transporte:

Esta capa, la más alta del stack, divide los "payloads" en bloques de bits a los que agrega un encabezamiento, dando origen a los **SEGMENTOS**. Cada segmento se numera con el fin de facilitar el reensamblaje en el destino

Unidades de datos en la capa de Red o Internetwork:

Agrega a cada segmento un encabezamiento con información que será útil durante el transporte del bloque de datos, como por ejemplo las direcciones IP de los computadores de origen y destino. Cada segmento, con el encabezamiento que agrega esta capa corresponde a un **PAQUETE**

Unidades de datos en la capa de enlace de datos:

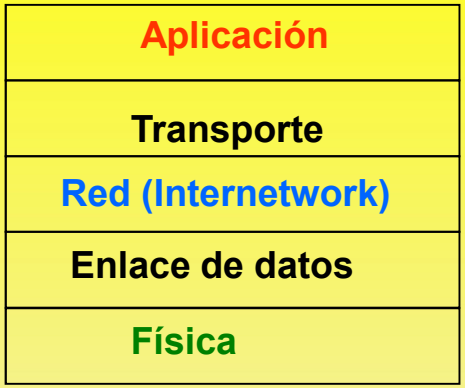
Esta capa del stack, forma las **TRAMAS**, agregando a cada paquete un encabezamiento con las direcciones MAC (Media Access Control address) de ambos computadores.

Las direcciones MAC, no modificables y únicas para cada dispositivo de hardware, permiten a los host en el lado receptor identificar las tramas dirigidas a ellos.

Datos en la capa física:

En la capa física los datos se transmiten convirtiendo las unidades de datos llamadas tramas, en impulsos eléctricos u ondas electromagnéticas y viceversa.

RESUMEN UNIDADES DE DATOS (PDU) [1] EN LAS DIFERENTES CAPAS TCP/IP



- Aplicación → Ejs.: PROTOCOLOS TELNET, FTP, HTTP, SMTP
- Transporte → Ejs.: PROTOCOLOS TCP, UDP
- Red (Internetwork) → Ej.: PROTOCOLO IP
- Enlace de datos → Ejs.: PROTOCOLOS ETHERNET, TOKEN RING, FDDI, X.25, WIRELESS, ASYNC, ATM, SNA

		PDU
Capa de aplicación	Protocolos Tel IP	Payload (datagrama)
Capa de transporte	TCP ó UDP	Segmento
Capa de red o Internetwork	IP	Paquete
Capa de enlace de datos	Ethernet	Trama
Capa física :		Bits en forma de impulsos eléctricos, ondas electromagnéticas, luz

(1) PDU = Protocol Data Unit

3.3.4 Principales semejanzas y diferencias en los modelos OSI y TCP/IP

Semejanzas

- El modelo OSI, al igual que el modelo TCP/IP se basa en el concepto de pilas o “stack” de protocolos independientes.
- Las funcionalidades de las capas OSI y TCP/IP son bastante parecidas
- En ambos modelos las capas de transporte y superiores proporcionan un servicio independiente de extremo a extremo
- Ambos modelos definen capas de red, de transporte y de aplicación

Diferencias

- El modelo OSI distingue claramente la diferencia entre los conceptos Servicios, Interfaces y Protocolos. En TCP/IP ello no ocurre así.

- El número de capas en OSI es 7 mientras que en TCP/IP es solamente 5

- Modos de conexión en la capa de transporte

  En la capa de transporte el modelo OSI tan solo acepta comunicaciones orientadas a la conexión.

  El modelo TCP/IP en la capa de transporte soporta tanto comunicaciones orientadas a la conexión como no-orientadas a la conexión (protocolos TCP y UDP respectivamente).

- Modos de conexión en la capa de red

  En la capa de red el modelo OSI soporta comunicaciones tanto orientadas a la conexión como no-orientadas a la conexión

  El modelo TCP/IP en esta capa tan solo acepta comunicaciones no-orientadas a la conexión.

3.3.5 Protocolos de capa transporte en modelo TCP/IP

- Para enviar los payload desde el origen al destino, los programas que constituyen la aplicación, se comunican peer to peer.

- Para ello, en cada extremo acceden a sus respectivos stack de protocolos

- La comunicación se hace con el apoyo de uno de dos posibles protocolos que forman parte del stack de protocolos y que proporcionan servicio de transporte a la aplicación:

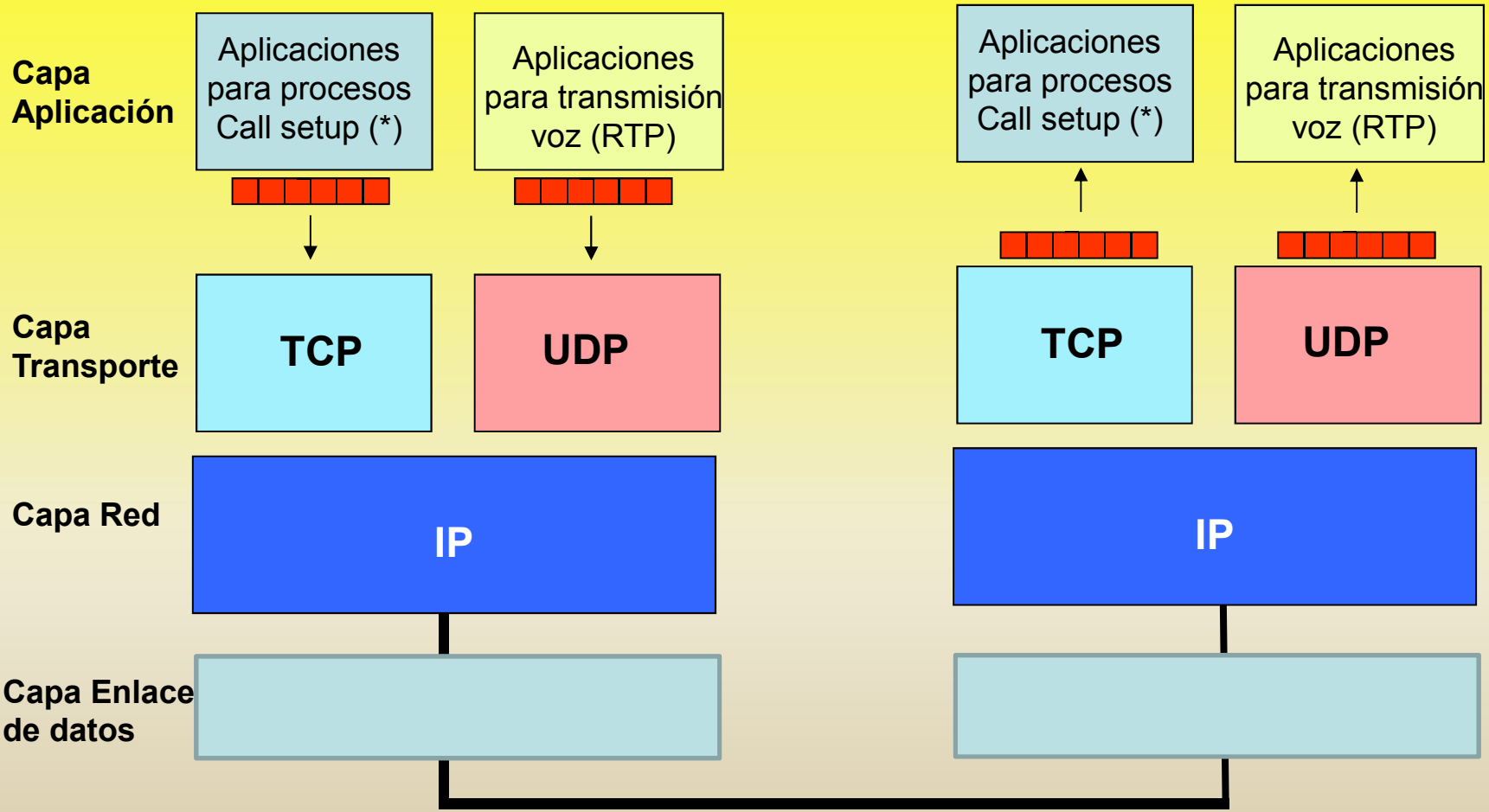
  TCP: Transmission Control Protocol

  UDP: User Datagram Protocol

- En el año 2000 el IETF definió un nuevo protocolo para la capa de transporte llamado Stream Control Transmision Protocol (**SCTP**)

Si la aplicación privilegia **seguridad** y **confiabilidad** se utiliza **TCP**

Si la aplicación privilegia **rapidez** se utiliza **UDP**



(*) también llamados de “señalización”

3.3.5.1 TCP

- Cuando la aplicación invoca el protocolo Transmission Control Protocol (TCP), es porque el programa de envío requiere certeza de que el programa de recepción reciba correctamente toda la información enviada

- Es decir se quiere evitar lo más posible que durante el transporte los datos se pierdan, dupliquen o dañen

- TCP: ambos extremos que intercambian datos mantienen un estricto control de todo lo que se envía y recibe. TCP establece una conexión virtual duplex (a nivel de capa de transporte) entre dos puntos definidos por su dirección IP y el nº de puerto TCP.

- TCP garantiza el transporte confiable extremo-extremo. Normalmente los browser en los computadores personales se comunican con el programa del servidor web utilizando interfase TCP cuando buscan páginas web, ya que en este caso si todos los datos no llegan intactos aparecerían hoyos o partes de datos fuera de orden en la pantalla, lo que es inaceptable. Controla secuencia.

- En resumen: la aplicación decide usar TCP cuando requiere certeza de que el extremo receptor reciba correctamente todo lo que envíe el extremo enviador

Más información: http://www.networksorcery.com/enp/protocol/tcp.htm

La filosofía básica del protocolo TCP

Cada vez que la capa TCP de la unidad de origen envía un segmento de datos, inicia un temporizador. Cada segmento tiene un campo con el correspondiente número de secuencia.

Al ser recibido OK el segmento en la unidad de destino, la capa TCP receptora devuelve a la transmisora otro segmento de datos que tiene por finalidad confirmar la recepción de éste.

El segmento de confirmación puede o no encapsular paylod, pero siempre incluye un campo con un número que corresponde al número secuencial del segmento que el receptor está esperando recibir (es el n° de segmento siguiente al último que recibió OK).

Si el temporizador de la unidad de origen expira antes de haber recibido la confirmación, el origen vuelve a enviar el mismo segmento.

De esta forma gracias a la capa TCP el modelo TCP/IP permite establecer conexiones a nivel de capa de transporte (canales lógicos), con lo que se asegura el intercambio eficiente y confiable de la información entre origen y destino, aún cuando la capa de red (capa IP) sea poco confiable ya que ella tan solo entrega servicio de capa de red no-orientado a la conexión (datagramas).

3.3.5.2 UDP

- Cuando la aplicación no requiere plena certeza de que todo lo que se envía será recibido (por Ej. cuando la información es suficientemente redundante), bastará invocar el protocolo User Datagram Protocol (UDP)
- UDP es un protocolo no orientado a la conexión. Provee tan solo checksum y multiplexaje de puertos. En este caso: payload = datagrama
- Cuando se utiliza este protocolo ninguno de ambos lados recibe confirmación de la recepción de los datos para asegurarse que todo llegó bien
- UDP es un protocolo de transporte rápido pero menos confiable y seguro
- El caso típico en que se usa UDP es para la transmisión de información de refresco de un contador en el extremo inferior de la pantalla de los computadores personales. En estos casos si se pierde un datagrama no es catastrófico porque pronto llegará otro
- En resumen: la aplicación decide usar UDP cuando es prioritaria la velocidad de envío y no se requiere asegurar que el extremo receptor reciba todo lo que envíe el extremo enviador, porque la información contiene suficiente redundancia que permite reconstruir lo perdido

Más información: http://www.networksorcery.com/enp/protocol/udp.htm

3.3.5.3 SCTP

- El protocolo **S**tream **C**ontrol **T**ransmission **P**rotocol fue definido en el año 2000 por el grupo SIGTRAN de IETF

- Al igual que TCP, es un protocolo para la capa de transporte que provee seguridad de que durante la transferencia de datos habrá pocos errores, al tener control de flujo y secuenciación, con ciertas ventajas de SCTP sobre TCP.

- Fue diseñado para transportar la información que contienen los mensajes SS7 usados en la PSTN, por redes de datos IP (Protocolo SIGTRAN)

- Es un protocolo que combina las ventajas de TCP y de UDP

- Está especificado en RFC 3286 y RFC 2960 del IETF

Más información: www.sigtran.org, www.sctp.de, www.ietf.org

3.3.6 Protocolo de capa de red en TCP/IP: Protocolo IP

3.3.6.1 Introducción

El protocolo de red Internet Protocol (IP) del modelo TCP/IP, es un protocolo no-orientado a la conexión.

La capa de red IP agrega a los SEGMENTOS recibidos de la capa de transporte un encabezamiento, creando así los PAQUETES.

Se encarga de enrutar por la red, en modo datagrama, los paquetes

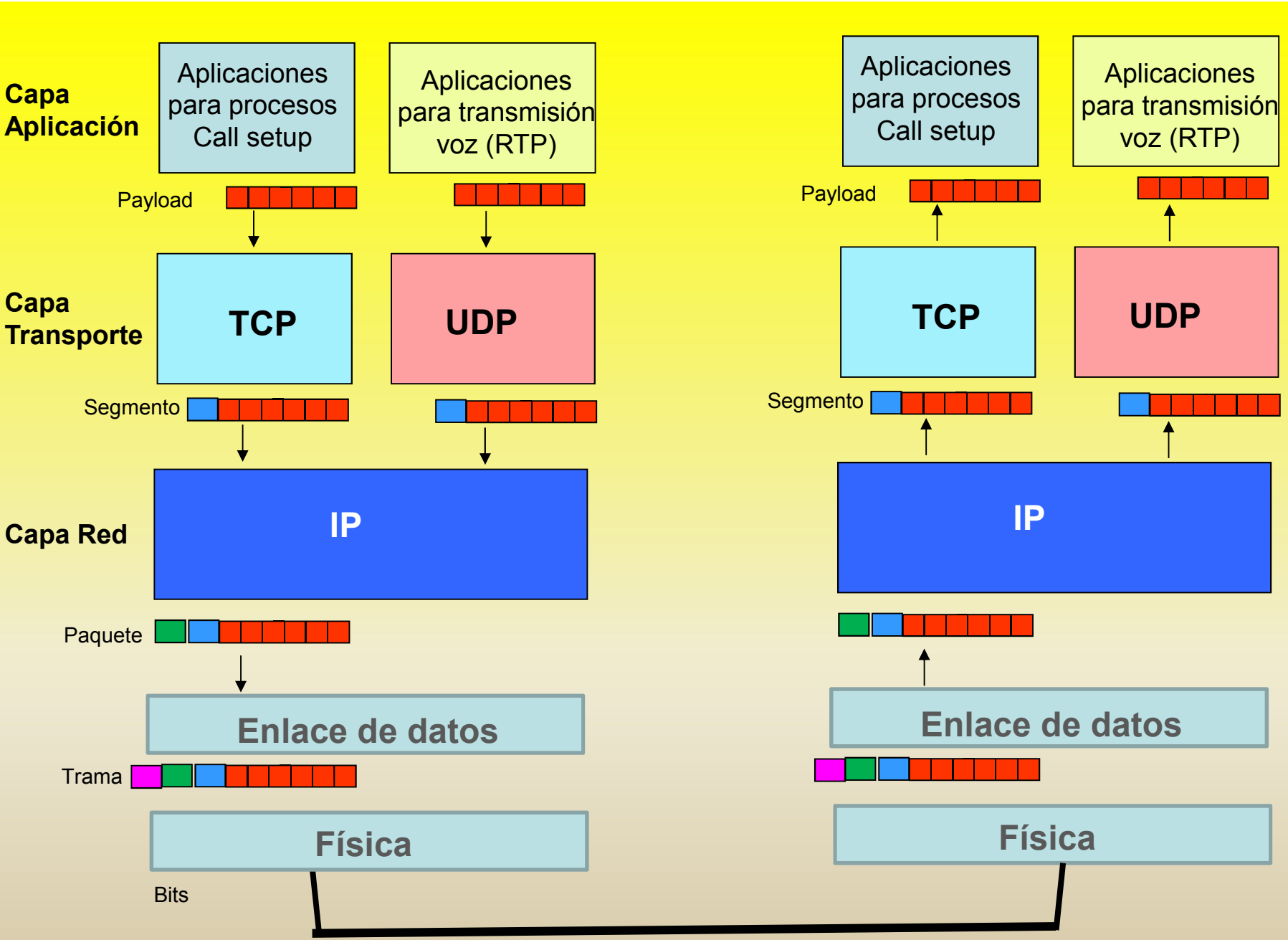
Como hemos visto

- Los programas de aplicación entregan porciones de datos (payload), a los que el stack de protocolos agrega encabezamientos (headers) correspondientes a las diferentes capas.
- El payload queda anidado en la unidad de la capa de transporte (UDP ó TCP), y a su vez el segmento UDP ó TCP queda anidado en la unidad de la capa de red, a la que se denomina paquete IP
- El header de paquete (capa de red IP), en el campo “checksum y protocolo” indica qué protocolo debe utilizarse para decodificar los datos que constituyen el payload (UDP o TCP)
- El header de paquete (capa de red IP) contiene la información necesaria para que el paquete “viaje” correctamente por la red. Entre la información que contiene destacan las direcciones de origen y destino del paquete

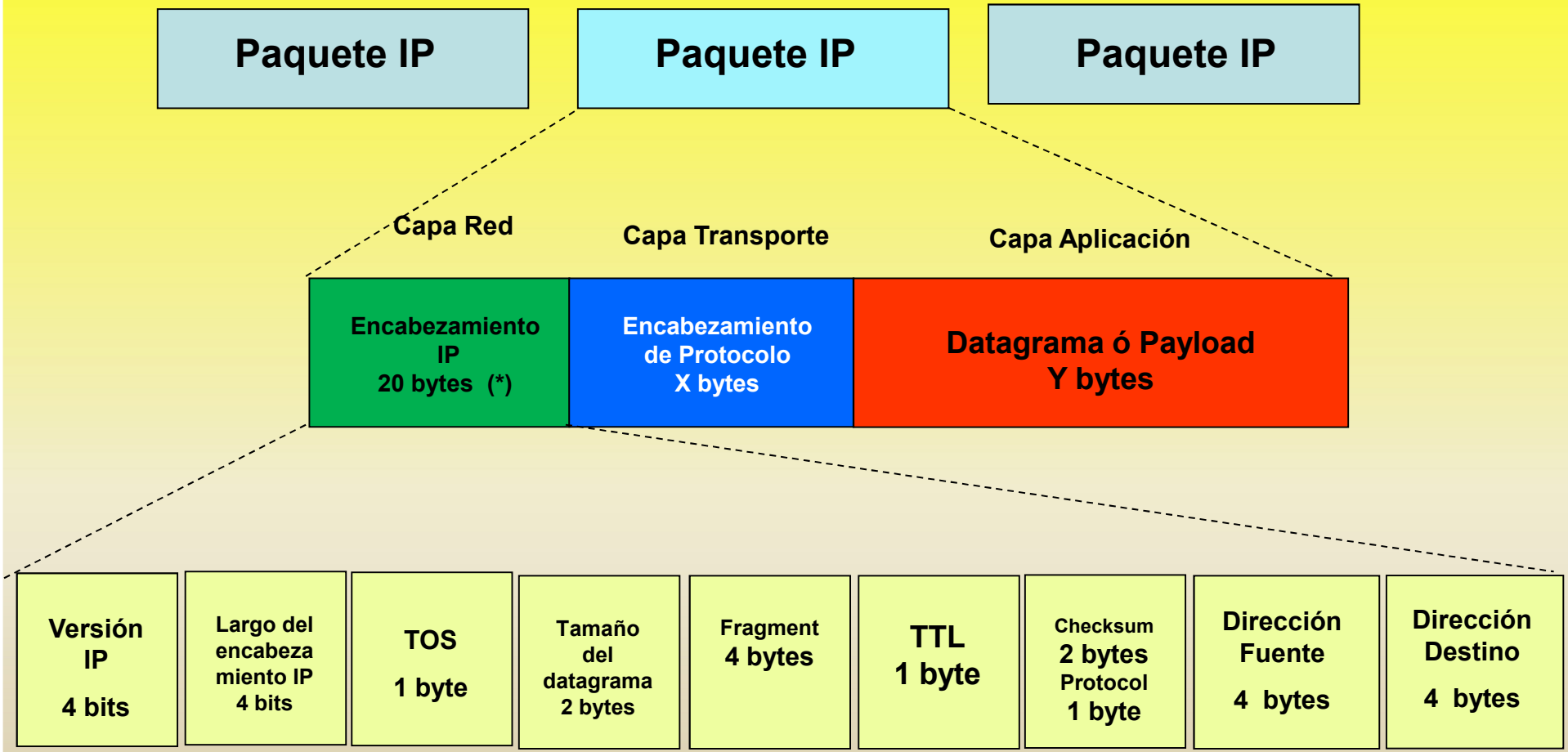
3.3.6.2 Estudio del encabezamiento en los paquetes IP

- En las próximas transparencias estudiaremos cómo está formado el encabezamiento que la capa de red (IP) agrega a los segmentos generados en la capa de transporte, para formar los paquetes IP.

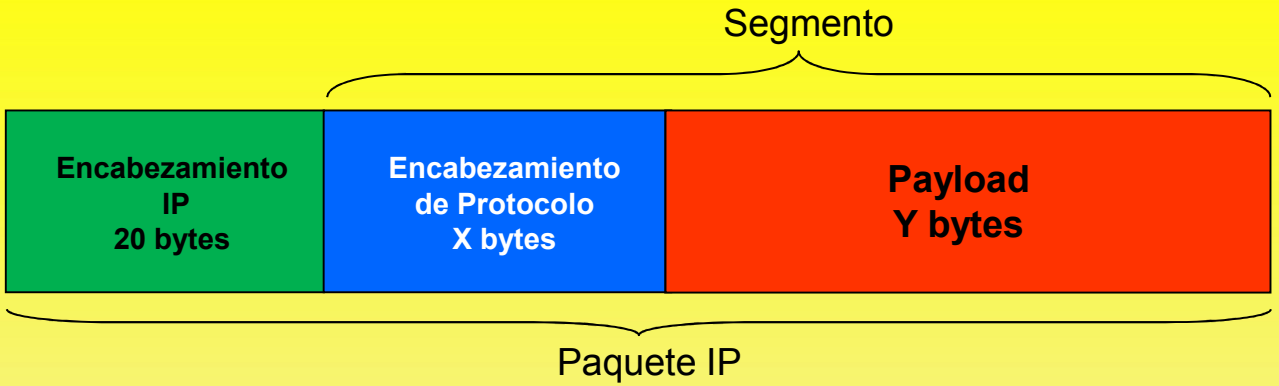
- La información que la capa de red incorpora en estos encabezamientos, es fundamental para el enrutamiento de los paquetes que hacen los routers, así como para que el extremo receptor pueda reconstituir la información original.


Capa Aplicación
Aplicaciones para procesos Call setup
Aplicaciones para transmisión voz (RTP)
Payload
Capa Transporte
TCP
UDP
Segmento
Capa Red
IP
Paquete
Enlace de datos
Trama
Física
Bits
Aplicaciones para procesos Call setup
Aplicaciones para transmisión voz (RTP)
Payload
TCP
UDP
Segmento
IP
Enlace de datos
Física

Paquetes IP y formato de su encabezamiento



Nota (*) Existe la opción de agregar bytes al encabezamiento



- Cada paquete IP tiene a lo menos 20 bytes que constituyen el “encabezamiento IP” (header). Además el encabezamiento puede tener entre 0 y 40 bytes adicionales en el campo “opciones”.

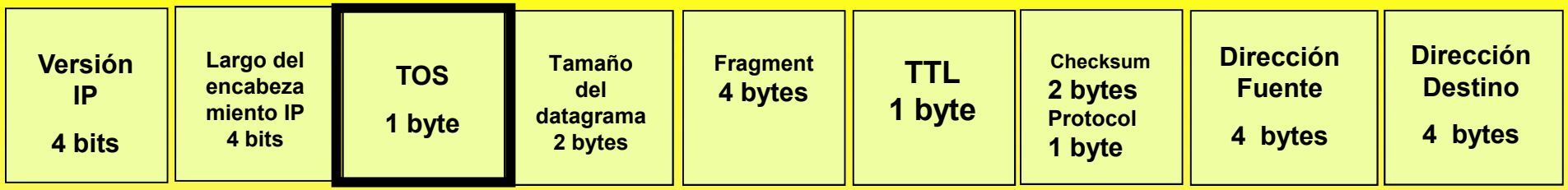
- Cada paquete IP anida un segmento, con el respectivo encabezamiento de protocolo puesto por la capa de transporte. Este encabezamiento lo pone la capa TCP ó la capa UDP.

- Los campos del “encabezamiento IP” (header) de cada paquete IP son estándares, independientemente de si anida información en protocolo TCP o UDP

Una forma didáctica de revisar los principales procesos en la transmisión de la información en forma de paquetes por la red de datos, y el efecto de dichos procesos sobre la voz paquetizada que se transmite cuando se tiene una comunicación de telefonía IP, es analizando los campos del encabezamiento IP.

Veamos los campos del encabezamiento IP

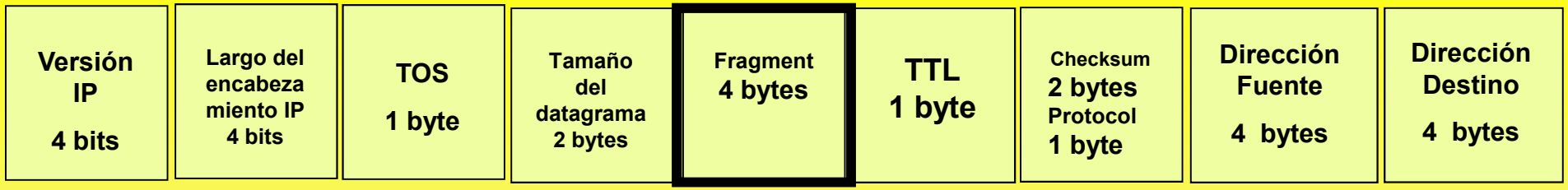
Encabezamiento IP



Campo TOS (Type of Service)

- Este campo tiene 1 byte y puede ser usado para marcar prioridad al paquete.
- Normalmente está puesto en cero. Cuando tiene valor cero significa que el dispositivo de la red que examina el paquete debe hacer el mejor esfuerzo para que éste llegue a su destino
- Sin embargo alguna aplicación podría poner este byte en valor distinto a cero, para por ejemplo requerir un manejo preferencial del paquete, solicitando una mínima probabilidad de pérdida o un mínimo retraso en su procesamiento
- El campo TOS es conocido como el Campo de Servicios Diferenciados (Differentiated Services ó DiffServ).
- La idea era que el router considere la información TOS antes de elegir, por ejemplo, un enlace satelital con mucho retardo. En la práctica no se usa así.

Encabezamiento IP



Campo Fragmentación y Reensamblaje

- Cada red fija el tamaño máximo para los paquetes que por ella se transmiten, lo que queda determinado por el parámetro MTU de la red (Unidad de Transferencia Máxima) Ejs.: Ethernet = 1.500 octetos; Token ring = 4.500; X.25 = 256; Frame Relay = 8.192
- Entonces a veces es necesario fragmentar. Se fragmenta el segmento y se repite el encabezamiento en cada paquete que lleva fragmento del segmento
- Dentro de este campo se distinguen 3 bits para un flag que toma el valor “more” cuando se quiere indicar que a continuación vienen más fragmentos. Cuando tiene el valor “DF” (don´t fragment) se debe preferir descartar el paquete antes que fragmentarlo
- Dos bytes de este campo son la “identificación”. Todos los paquetes con fragmentos de un mismo segmento original tienen la misma identificación
- Hay una parte llamada “offset del fragmento” que indica su posición relativa en el segmento original

FRAGMENTACION IP

Cuando un router recibe un paquete más largo que la MTU del próximo enlace, tiene dos opciones:

- Desechar el paquete y enviar un mensaje ICMP (Internet Control Message Protocol) indicando error: “Paquete demasiado largo”

- Fragmentar el paquete de modo que el tamaño de los fragmentos enviados al próximo enlace sean menores que su MTU

Los procedimientos para la fragmentación IP, transmisión y reensamblado son descritos en RFC 791.

La RFC 815 describe un algoritmo simplificado para reemsamblar.

El reensamblado puede realizarse en el computador de destino, pero también puede ocurrir en un router intermedio

Si el computador de destino recibe un paquete IP dividido en fragmentos, la capa IP deberá reensamblarlo, para entregar un solo segmento a la capa superior.

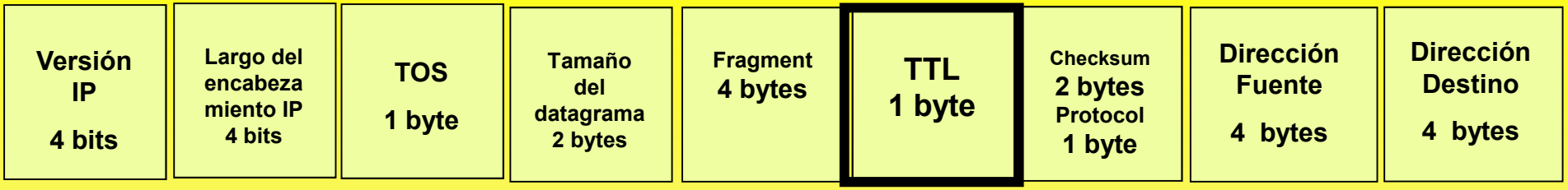
Cuando se usa protocolo orientado a la conexión, como lo es el TCP, la fragmentación IP puede causar excesiva retransmisión de paquetes por la red. En efecto, en este caso, cuando se pierde un solo fragmento de paquete, TCP debe retransmitir todos los fragmentos.

Por esta razón es necesario optimizar el tamaño de los paquetes a enviar por la red. Normalmente se usa uno de los dos criterios siguientes para decidir el tamaño de los paquetes que envía el computador fuente:

- El computador fuente envía paquetes de largo igual a la MTU del primer enlace hacia el computador de destino

- Se investiga la MTU hacia el computador de destino, que determina el largo de los paquetes de modo de evitar fragmentación. Esto se hace de acuerdo a la RFC 1191, mediante el proceso llamado “Path MTU Discovery”

Encabezamiento IP



Campo TTL (Time To Live)

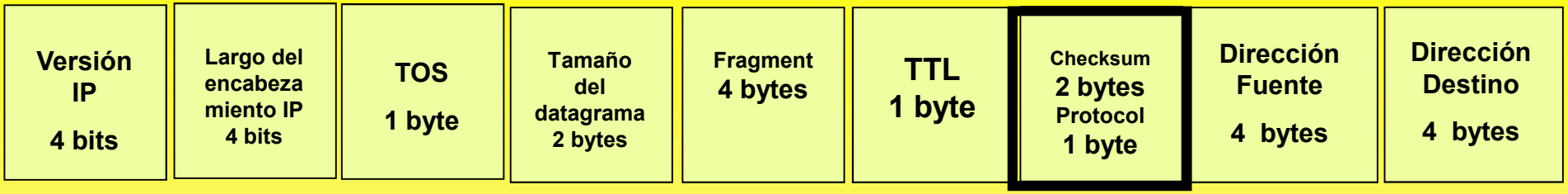
- Cada vez que un paquete completa un salto durante su viaje por la red, se reduce en 1 el valor de este byte. También se decrementa durante las esperas largas en buffers.

- Si un dispositivo recibe un paquete con TTL = 0, es indicación de que ese paquete debe ser descartado.

- Es decir TTL = 0 significa que el paquete ha superado la vida que le fue asignada (debido a que tuvo muchos saltos), lo que es indicador de que existe un problema con la red o con el paquete.

- De esta forma TTL evita que algunos paquetes queden eternamente circulando por la red.

Encabezamiento IP



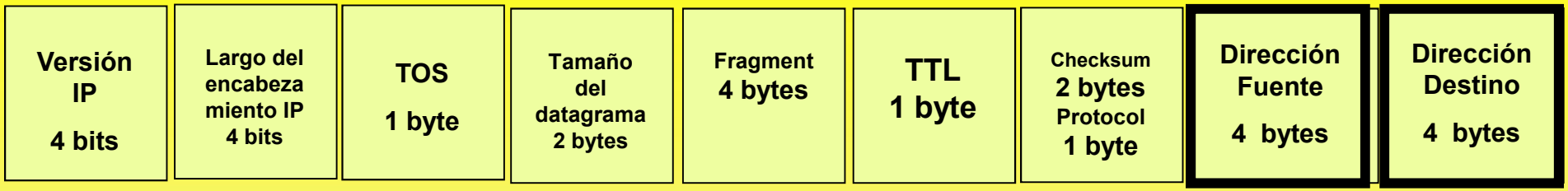
Campos Protocolo y Checksum

- Protocolo: especifica el protocolo encapsulado (ej. TCP = 6; UDP = 17)
- Se usa un checksum con el fin de detectar cambios en los bits del encabezamiento, provocados por problemas en los dispositivos de la red durante la transmisión. Estos cambios pueden ser accidentales o maliciosos
- El lado que envía aplica a los bits del encabezamiento que se está enviando una fórmula y escribe el resultado final de ella en el campo checksum
- El lado receptor también hace lo mismo con los bits que recibe
- Si el checksum coincide con el recibido, hay seguridad que no hubo cambio en los bits durante la transmisión
- En caso contrario se descarta el paquete recibido

El objetivo del checksum del encabezamiento es proporcionar una protección básica frente a corrupción de datos

El checksum del encabezamiento se calcula solo para los bytes del encabezamiento, con los bytes del campo checksum puestos en cero

Encabezamiento IP



Campos Dirección Fuente y Dirección Destino

- Corresponden a las direcciones IP de las aplicaciones de origen y de destino. Cada dirección tiene 4 bytes.

- Tradicionalmente se utiliza una notación que incluye puntos para separar los 4 bytes, por ejemplo 199.72.46.202

Direcciones IP

- **Dirección de 32 bit, escrita como cuatro números decimales separados por puntos (un número decimal por byte) Ejemplo: 155.34.60.112**

- **Estructura de direccionamiento jerárquico**
  - **Dirección de la red/ Dirección del Host/ Puerta (Port ID)**
  - **La dirección completa se llama socket**
  - **La dirección de red y la dirección de host se transporta en el encabezamiento IP**
  - **La puerta (Port ID que indica sending process) se transporta en el encabezamiento TCP. Es decir el port correspondiente al proceso de envío está en el encabezamiento de segmento.**

Campo Opciones

Adicionalmente a los campos descritos, el encabezamiento IP puede tener un campo “opciones”.

Se definieron varias opciones, cada una de las cuales se identifica empezando con un código de 1 byte que la identifica.

Las opciones son de longitud variable.

Opciones definidas:

Seguridad: Especifica el nivel de reserva de la información

Enrutamiento estricto: Obliga a que el paquete se enrute desde origen a fin siguiendo una ruta exacta especificada como sucesión de direcciones IP. Se usa durante el mantenimiento en emergencias en que se han dañado tablas en algunos routers o para medir tiempos.

Registrar ruta: Hace que todos los routers a lo largo de la ruta agreguen en el campo opción su dirección IP, con el fin de diagnosticar problemas de enrutamiento

Marca de tiempo: Igual a opción registrar ruta, pero además cada router deja un marca de tiempo

4 CALIDAD DE SERVICIO (QoS) EN REDES TCP/IP

En este capítulo revisaremos algunos fenómenos que ocurren durante el transporte de los paquetes por las redes TCP/IP. Como veremos, estos provocan degradación de la calidad en los servicios en tiempo real, como lo es el servicio de telefonía IP.

Estos fenómenos no afectan mayormente la calidad de los servicios que no son en tiempo real, como lo es la transmisión de e-mails y de archivos por la red de datos.

4.1 Sensibilidad del oído humano a las distorsiones que introduce la transmisión de la voz

El oído humano es particularmente sensible a

- los retardos de la voz: provoca “eco” y efecto “walkie talkie”
- las irregularidades del ritmo verbal y
- las pérdida de sonidos.

EFECTOS DEL RETARDO SOBRE LA CALIDAD DE LA COMUNICACIÓN

- En una conversación telefónica retardos de la voz iguales o superiores a 150 mseg. (en un sentido) son notorios y poco aconsejables.
- Retardos de la voz mayores a 300 mseg. son molestos.

TIPOS DE CALIDAD EN UNA CONVERSACIÓN TELEFÓNICA SEGÚN EL RETARDO DE LA VOZ

Se tipifica la calidad de diferentes tipos de comunicaciones, según los tiempos de retardo aceptados.

	Máximo retardo para la voz (un solo sentido)
CALIDAD VOZ ó CALIDAD TELEFONÍA:	0 - 150 mseg.
CALIDAD SATELITAL:	160 - 500 mseg
CALIDAD BANDA CIUDADANA:	400 - 700 mseg.
CALIDAD FAX Y TRANSMISIONES BROADCAST:	450 - 800 mseg.

Se tiene entonces que para tener "calidad voz" en telefonía IP, todos los procesos IP deben realizarse dentro de los 150 mseg. de retardo a que se han acostumbrado por años los usuarios telefónicos.

4.2 Retardo y Latencia en redes TCP/IP

Los procesos a que va siendo sometida la información durante su viaje por la red provocan retardos.

En redes informáticas de datos se denomina **latencia** a la suma de los retardos temporales dentro de una red.

Los retardos son producidos por las demoras propias de la transmisión de los paquetes por la red, por los tiempos de procesamiento y por los tiempos de espera en buffers.

La latencia se mide como el tiempo de tránsito promedio de un servicio desde la puerta de ingreso a la puerta de egreso de la red.

- Los mayores responsables de la latencia son los procesos de DIGITALIZACION, PAQUETIZACION, SERIALIZACION, PROPAGACION EN LA RED (cantidad de “links” o “saltos” por los que pasan los paquetes), PROPAGACION INTERNA EN LOS COMPONENTES DE LA RED, COLAS EN BUFFERS (mientras los paquetes esperan su turno para ser procesados),

- La latencia afecta la calidad del servicio por sus efectos “walkie-talkie” y “eco”.

- El retardo tiene una componente fija y una variable. Esta última depende, por ejemplo, del camino que siguen para alcanzar su destino los paquetes durante su viaje por la red, o de los tiempos variables que permanecen haciendo cola en los buffers. Los retardos variables provocan el fenómeno llamado **VARIACION DE RETARDO**

- Respecto al retardo de propagación provocado por la red, la ITU-T en la Recomendación G.114 propone que cuando no se disponga de datos sobre este valor, se utilice en los cálculos un retardo de propagación de 6 microsegundos por Km.

4.3 Variación de retardo: Jitter y Wander

Si bien el fenómeno de retardo ya degrada la calidad del servicio de telefonía IP, ésta se degrada más aún cuando el retardo es variable.

Las variaciones del retardo pueden ser rápidas o lentas. En el primer caso la variación de retardo se conoce como “jitter” y en el segundo caso como “wander”

En una conversación telefónica cualquier irregularidad en la llegada de los paquetes (jitter, wander) es molesta para el que escucha.

Como veremos, la variación de retardo puede ser corregida, pero a costa de introducir más retardo.

- Las variaciones rápidas del retardo (variaciones de alta frecuencia) se conocen como JITTER, son provocadas principalmente por las colas de espera en buffers y son las que más afectan a la calidad del servicio.

- A las variaciones lentas se llama WANDER

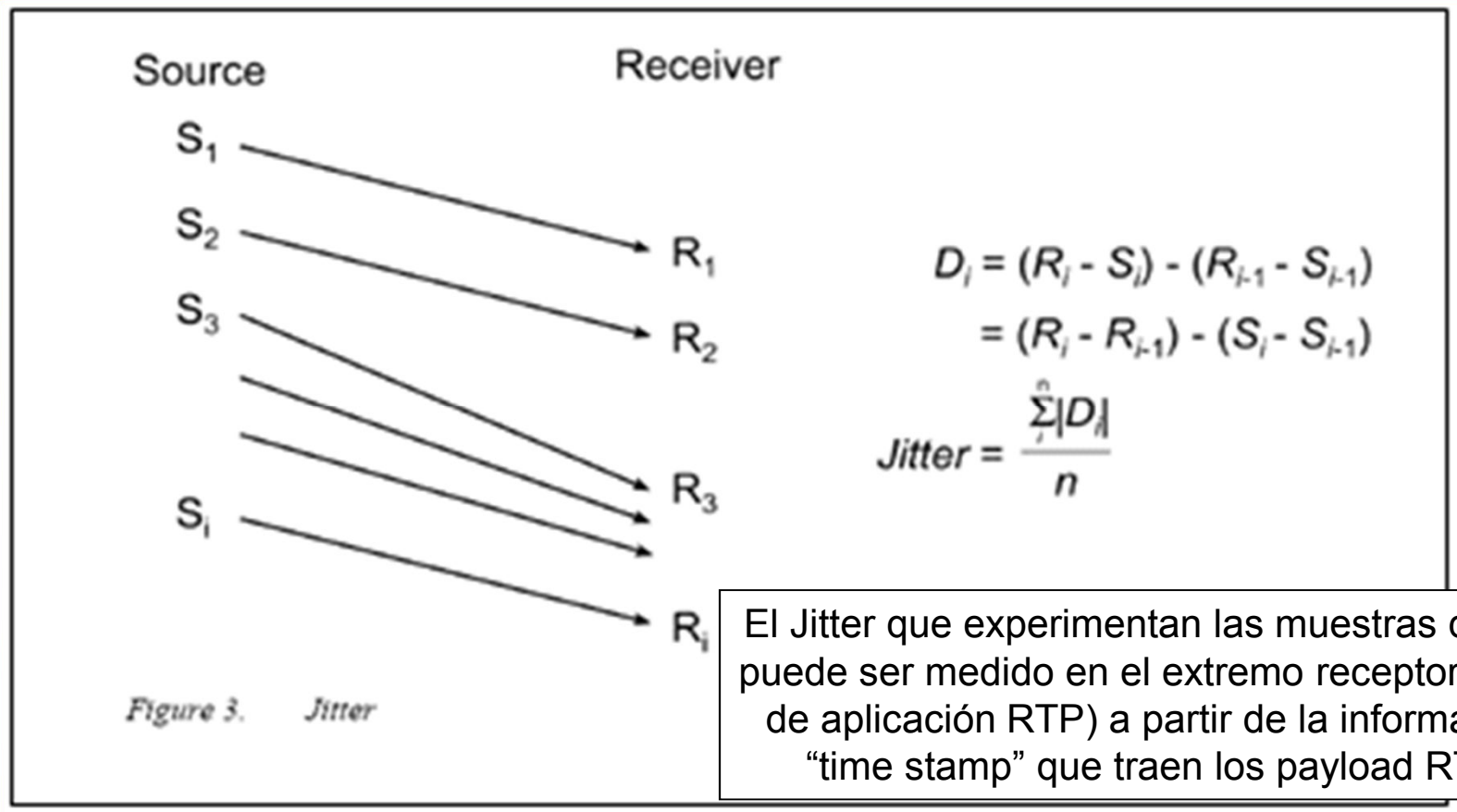


Figure 3. Jitter

El Jitter que experimentan las muestras de voz puede ser medido en el extremo receptor (capa de aplicación RTP) a partir de la información "time stamp" que traen los payload RTP

La forma utilizada para contrarrestar los efectos de la variación de retardo, es almacenar las tramas recibidas en un buffer suficientemente grande, que dé tiempo a que lleguen las tramas que han tenido mayor retardo y luego ordenar las tramas en la secuencia correcta antes de reenviarlas.

Es decir se logra corregir la variación de retardo, pero a costa de introducir retardo adicional.

Si la variación de retardo es grande se requiere mayor tiempo de buffering. Si la variación de retardo es menor, se requiere menor buffering. Por esta razón, con el fin de disminuir el retardo adicional introducido, se usa un “buffer jitter adaptivo”.

El buffer jitter adaptivo permite ajustar el tiempo de almacenamiento de las tramas en el buffer de destino, a la cantidad de jitter que está ocurriendo en la red, cantidad que entre otros factores depende del tráfico que instantáneamente presiona sobre la red.

Generalmente, para efectos de los cálculos, se considera que el retardo que introduce la corrección de jitter es igual a 2 veces el período R entre datagramas.

4.4 Pérdida de paquetes

La pérdida de paquetes en el trayecto extremo-extremo, provoca como efecto pérdidas de sonidos, que también son muy molestas al oído humano.

La calidad de la voz se hace intolerable por pérdida de sonidos, si la pérdida de paquetes extremo-extremo supera 3%

Normalmente se acepta hasta un 1% de pérdida de paquetes, aunque es preferible que ésta no sobrepase 0,5%.

No siempre es fácil lograr este objetivo, si se tiene en cuenta que en las redes IP intencionalmente se eliminan paquetes para evitar congestiones de red. Al respecto, vimos algunos casos cuando estudiamos los campos del encabezamiento IP: Fragmentación y Reensamblaje, TTL y Checksum .

I_e = Impairment factor G.113 (Factor de deterioro)

Codec	Ie (0% loss)	Ie (2% random frame loss)	Ie (5% random frame loss)
G.711 without PLC	0	35	55
G.711 with PLC	0	7	15
G.729A	11	19	26*
G.723.1 (6.3 kbps)	15	24	32†

* The values were for 4% random frame loss. The values for 5% were not provided in the Appendix.
† The values were for 4% random frame loss. The values for 5% were not provided in the Appendix.

5	Very good
10	Good
20	Adequate
30	Limiting case
45	Exceptional limiting case
55	Customers likely to react strongly (complaints, change of network operator)

Packet Loss Concealment (PLC), es una técnica para enmascarar los efectos de la pérdida de paquetes en comunicaciones VoIP, que veremos más adelante