

IIE-425

Redes de computadores

Escuela de Ingeniería Eléctrica
Universidad de Costa Rica

Febrero, 2021

Clase 10

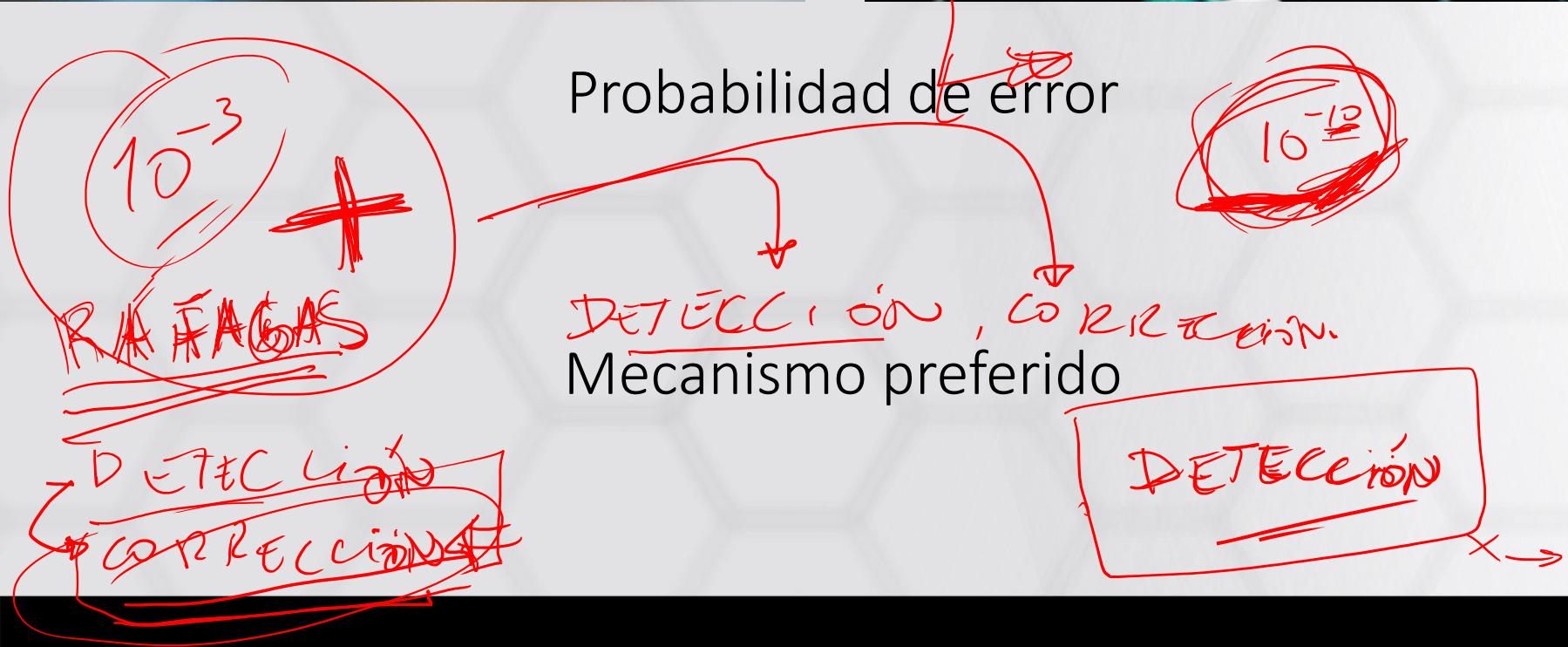


Objetivo

-Conocer los parámetros básicos a considerar en diseño de redes de computadores.



Detección y corrección de errores



Códigos de corrección de errores

- 1. Códigos de Hamming.
- 2. Códigos convolucionales binarios.
- 3. Códigos de Reed-Solomon.
- 4. Códigos de verificación de paridad de baja densidad.

La longitud de un bloque será $n = m + r$

m: tamaño del mensaje

r: redundancia del mensaje

Códigos (m,n) o tasa de código m/n (inf. no redundante)

(n,m)

*bits adicionales
corrección error.*

% cargo útil.

Distancia de Hamming

$$\begin{array}{l} A \\ B \\ C \end{array} \quad \begin{array}{r} 10001001 \\ 10110001 \\ \hline 00111000 \end{array}$$

$$A \xrightarrow{\text{XOR}} B = C$$

XOR entre palabras

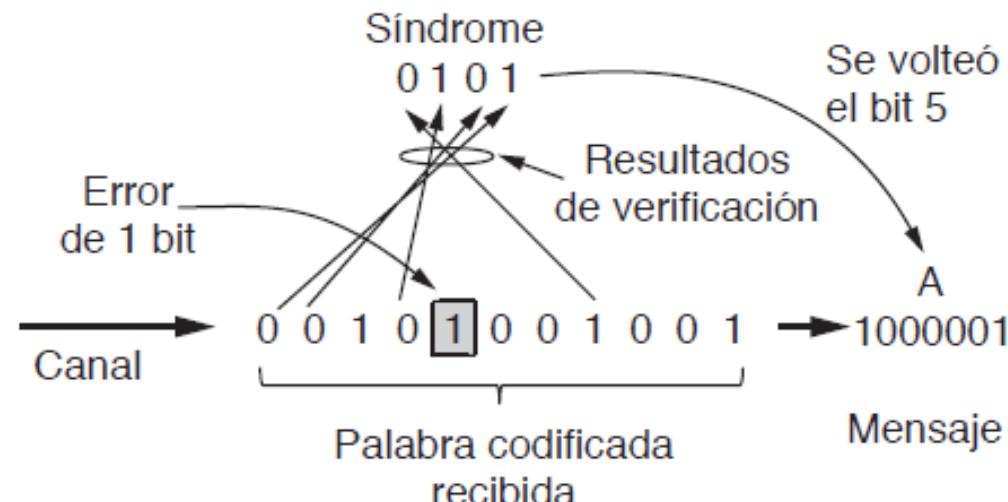
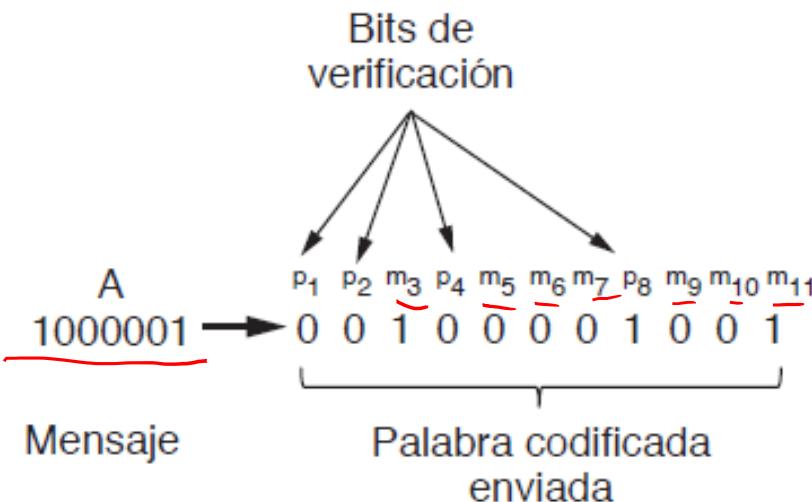
1	1	0	1	1	0	1	0
1	1	0	1	0	1	0	1
0	0	0	1	1	1	0	0
0	0	0	1	1	1	0	0
1	0	1	0	1	0	1	0
1	1	1	0	0	1	0	0

- Cantidad de bits diferentes entre palabras.
- Si dos palabras están separadas una distancia d , se requerirán d errores de un solo bit para convertir una en la otra.
- Para detectar d errores de manera confiable se necesita un código con distancia $d + 1$ \Rightarrow REDUNDANCIA
- Para corregir d errores se necesita un código de distancia $2d + 1$. \Rightarrow REDUNDANCIA.

$$\underline{(m)+(r)+(1) \leq 2^r} \text{ (relación de Hamming)}$$

Códigos de Hamming:

- Bits potencias de 2 (1, 2, 4, 8, 16, etc.) son bits de verificación (r bits).
- El resto (3, 5, 6, 7, 9, etc.) se rellenan con los m bits de datos



Relleno de bits

1 0 0 0 0 0 1

$m = 3$ bits

$$m + r + 1 \leq 2^r$$

$r = 1$

$$8 + 1 + 1 \leq 2^1 \times$$

$r = 2$

$$8 + 2 + 1 \leq 2^2 \times$$

$r = 3$

$$\cancel{8 + 3 + 1} \leq 2^3 \times$$

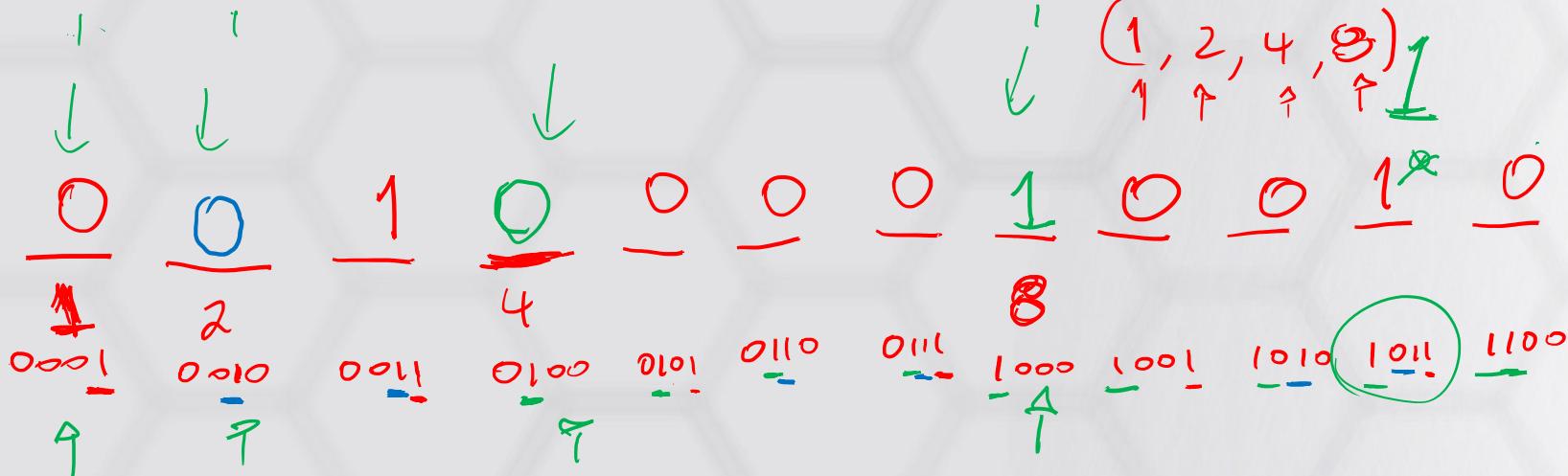
$r = 4$

$$8 + \cancel{4} + 1 \leq 2^4 \checkmark$$

1 0 0 0 0 0 1 0

$$\begin{array}{|c|} \hline m = 8 \\ \hline r = 4 \\ \hline \end{array}$$

$$\begin{array}{l} n = m + r \\ n = 12 \end{array}$$



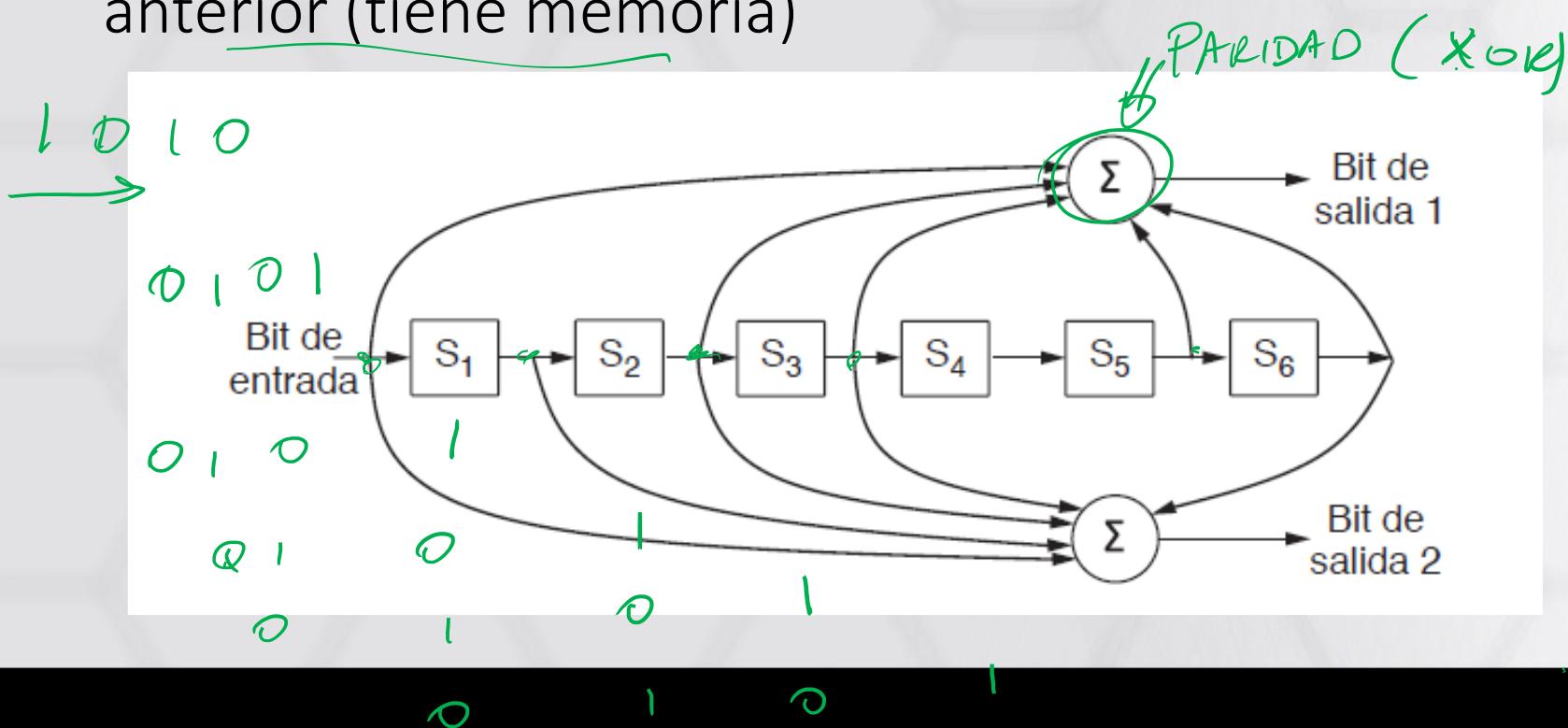
de mensaje.

- Valor de la posición k , se obtiene al reescribir k como la suma de las potencias de 2. Por ejemplo,
 $k_{11} = r_{1+2+8} = r_1 + r_2 + r_8 = 1$
- Errores en los bits (de mensaje) se corrigen en el receptor para coincidir con los bits de paridad

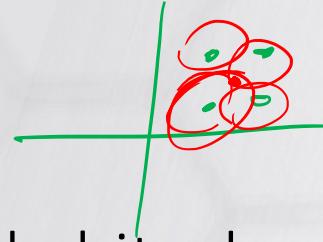
Redundancia

Código convolucional

- Se utiliza en sistemas GSM, satelitales y 802.11
- La salida depende de los bits de entrada actual y anterior (tiene memoria)



Código convolucional



- Para decodificar se busca secuencia de bits de entrada que tenga la mayor probabilidad de haber producido la secuencia de salida.
- Para códigos “pequeños” (k bajo) se utiliza algoritmo de Viterbi.

Código Reed-Solomon

- Se basan en que todo polinomio de n grados se determina en forma única mediante $n + 1$ puntos.
- Una línea, por ejemplo, se representa mediante dos puntos. Puntos extra de la línea son “redundantes” pero sirven para confirmar y corregir errores.
REdundancia
- Código (255,233) es muy utilizado, por ejemplo en DSL y Cable Módem para corregir errores de ráfaga.



Código LDPC

↓ ↓ ↓ ↓

- Low density – parity check
- Utiliza una representación matricial del código. Las palabras se decodifican con un algoritmo de aproximación que mejora de manera reiterativa con base en el mejor ajuste de los datos recibidos con una palabra codificada válida. Esto corrige los errores.
- Para tamaños grandes de bloques y tienen excelentes habilidades de corrección de errores que superan a las de muchos otros códigos
- Utilizado en 10 Gbps Ethernet

~~RÁPIDAS~~

Quiz #3 \Rightarrow 15-fel-21

TAREA #2 \Rightarrow 11 - fel - 21

Ejercicios



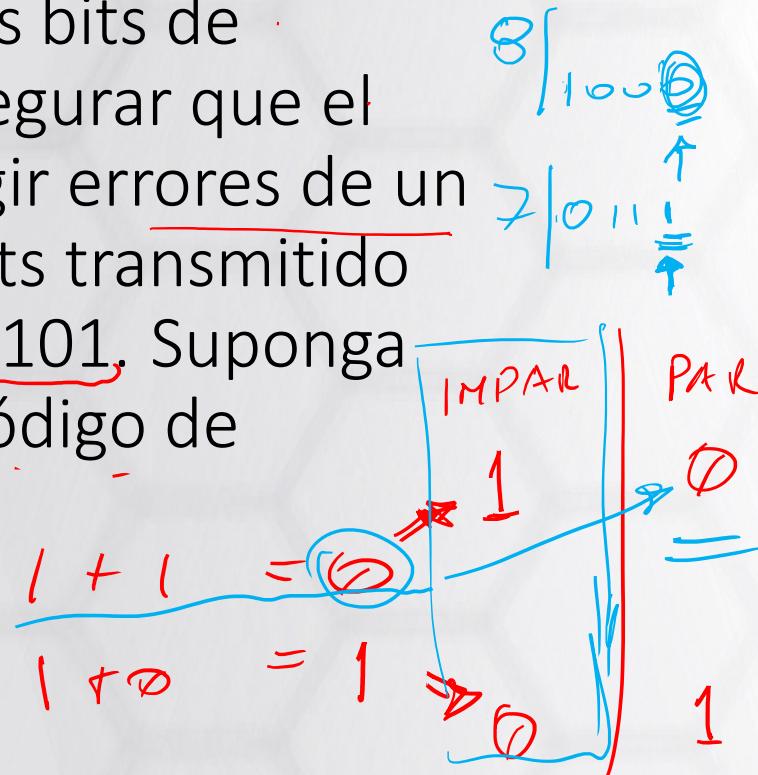
Ejercicio 9. Pág. 217

$$m+r+1 \leq 2^r$$

$$r = 5$$

- Se van a transmitir mensajes de 16 bits mediante un código de Hamming. ¿Cuántos bits de verificación se necesitan para asegurar que el receptor pueda detectar y corregir errores de un solo bit? Muestre el patrón de bits transmitido para el mensaje 1101001100110101. Suponga que se utiliza paridad par en el código de Hamming.

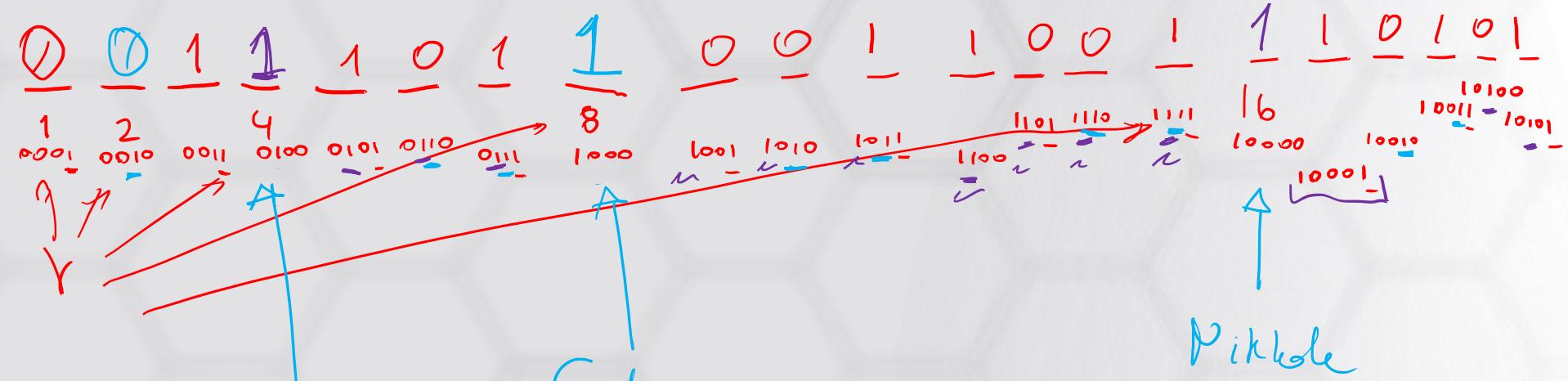
1, 2, 4, 3, 16



1101001100110101

Correction  Reception 

0 0 1 1 1 0 1 1 0 0 1 1 0 0 1 1 0 1 0 1



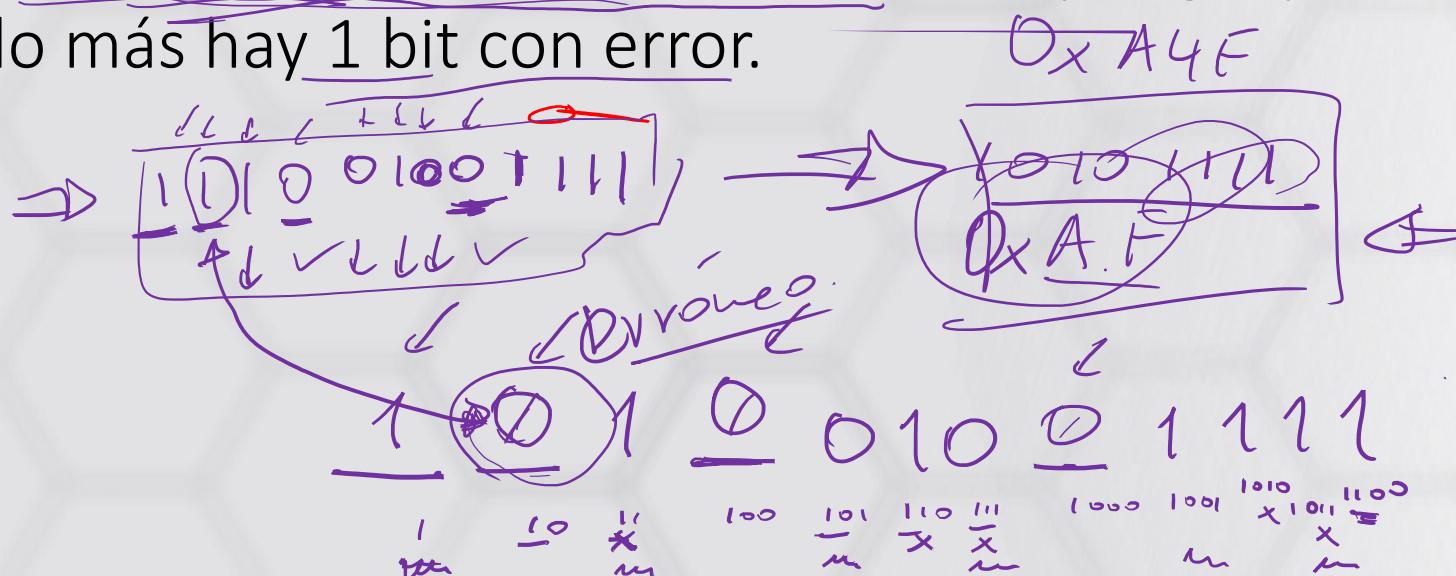
Colg

$$\begin{aligned}
 k_{17} &= r_{1+16} = r_1 + r_{16} \\
 &= 0 + 1 \\
 &= 1 //
 \end{aligned}$$

Pikkole

Ejercicio 10. Pág. 218

- Un código de Hamming de 12 bits, cuyo valor hexadecimal es 0xE4F, llega al receptor. ¿Cuál era el valor original en hexadecimal? Suponga que a lo más hay 1 bit con error.



Código de detección de errores



Códigos de detección

- Paridad ↗
 - Sumas de verificación ↗
 - Pruebas de redundancia cíclica (CRC) ↗
- (n, m)
↙ ↗
 n
↙ ↗
 m
↙ ↗
 $\%$

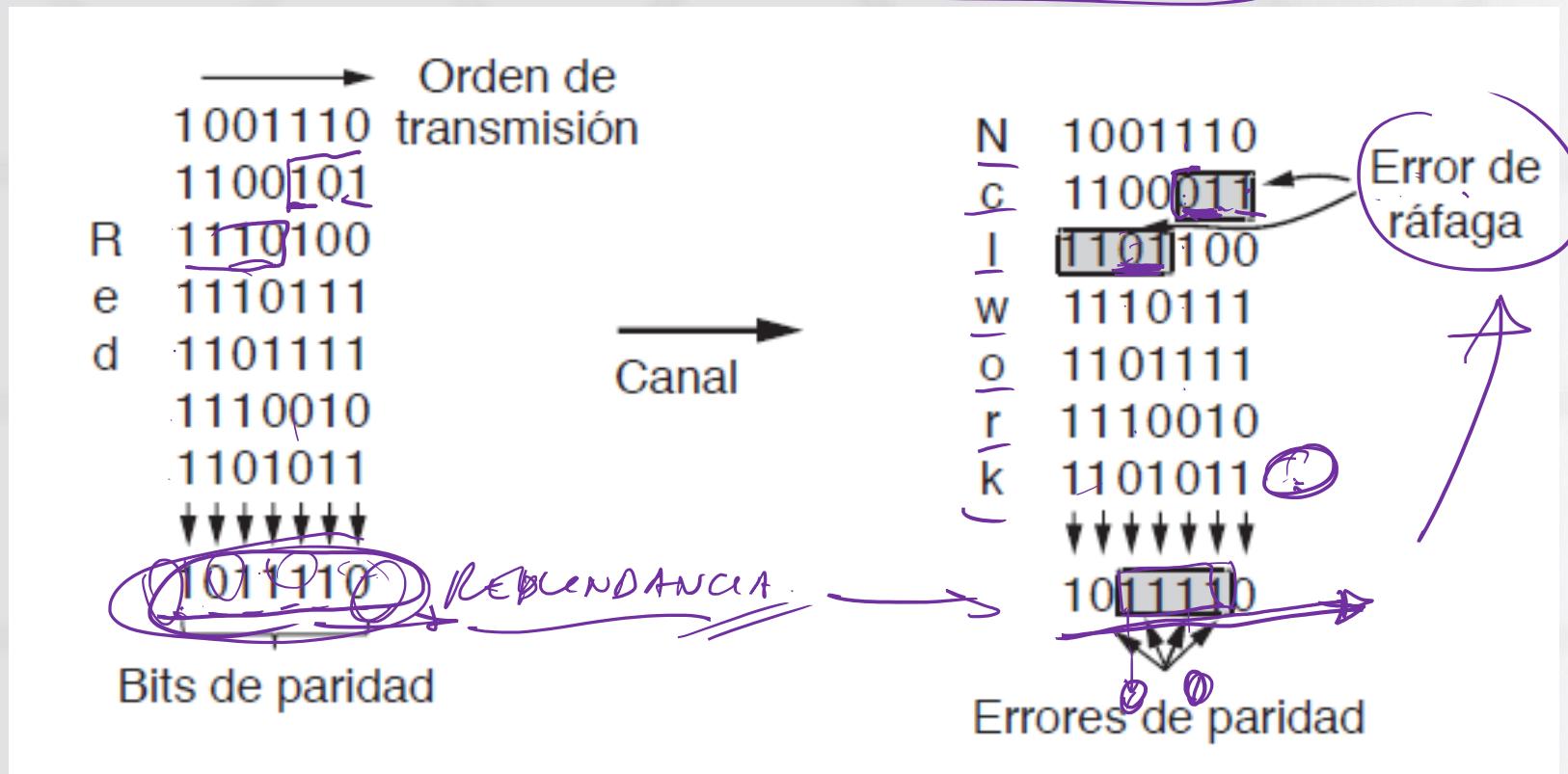
Bits de paridad

- Ejemplo más simple, se agrega un bit al final con la paridad de la palabra por transmitir:

1011010 -> 1011010 

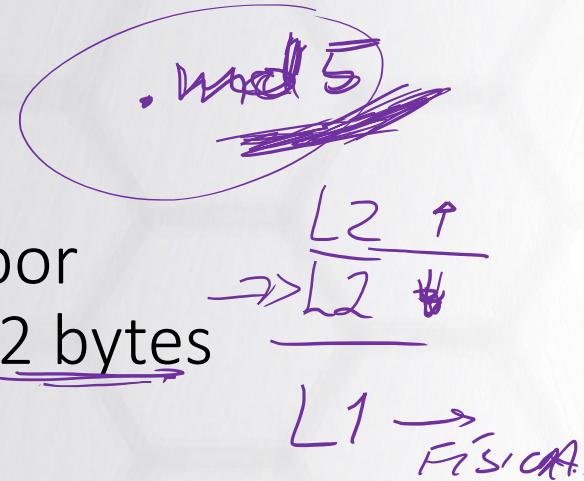
- Solo puede detectar error de 1 bit en la palabra
- No funciona para ráfagas, solo para tasas muy baja de errores en la transmisión

Intercalado Bits de paridad



Checksum (suma de verificación)

- Se utiliza ampliamente en otras capas, por ejemplo en protocolo IP (L3) se utilizan 2 bytes para suma de verificación.
- Este protocolo hace una verificación de palabras y no de bits. Puede detectar palabras con errores que hayan modificado su paridad.
- Método más confiable es la suma de Fletcher (1982) que incluye componente posicional



CRC

$$\sim \frac{1}{x^6} + \frac{0}{x^4+x^3} + \frac{1}{x+1}$$

polinomio

- También conocido como código polinomial
- Se obtiene el residuo de hacer la división (mediante XOR) entre polinomios. Si el residuo es 0 no hay errores en la transmisión.
- Ejemplo:

• D: Datos transmitidos 100100

• E: Datos adicionales para agregar divisibilidad 001 REDUNDANCIA

• Trama: 100100 001

• G: Generador 1101

• R: residuo

P E G
~~100100 001 / 1101~~

~~1101~~ | ~~11101~~
~~01000~~ |
~~1101~~ |
~~01010~~ |
~~1101~~ |
~~01110~~ |
~~1101~~ |
~~001110~~ |
~~1101~~ |
~~001110~~ |
~~1101~~ |
~~00000~~ R

CRC

$$\begin{array}{r}
 90513 \\
 9 \cdot 101 \\
 \hline
 023
 \end{array}$$

$$\begin{array}{r}
 10016 \\
 6 \downarrow \\
 40 \\
 \hline
 36 \\
 \hline
 4
 \end{array}$$

CRC

- Utilizado normalmente en algunos estándares de IEEE:

The diagram illustrates the polynomial representation of the CRC-32 generator polynomial. A red circle highlights the label $G_{\text{CRC-32}}$. To its right is the polynomial expression $x^{32} + x^{26} + x^{23} + x^{22} + x^{16} + x^{12} + x^{11} + x^{10} + x^8 + x^7 + x^5 + x^4 + x^2 + x^1 + 1$. Above the polynomial, the number 32 is circled in red. Below the polynomial, a red arrow points to the constant term '1' at the end of the expression.

$$G_{\text{CRC-32}} = x^{32} + x^{26} + x^{23} + x^{22} + x^{16} + x^{12} + x^{11} + x^{10} + x^8 + x^7 + x^5 + x^4 + x^2 + x^1 + 1$$

detecta todas las ráfagas con una longitud de 32 o menos bits y todas las ráfagas que afecten a un número impar de bits.

Ejercicios



Ejercicio 16. Pág. 218

- ¿Qué residuo se obtiene al dividir $x^7 + x^5 + 1$ entre el polinomio generador $x^3 + 1$?

Residuos ?

↓ ↓ ↓

Oxígeno Niklosen

Anílves

Ejercicio 17. Pág. 218



- Un flujo de bits 10011101 se transmite utilizando el método estándar CRC que se describió en el texto. El generador polinomial es $x^3 + 1$. Muestre la cadena de bits real que se transmite. Suponga que el tercer bit, de izquierda a derecha, se invierte durante la transmisión. Muestre que este error se detecta en el lado receptor. Mencione un ejemplo de errores de bits en la cadena de bits transmitida que no serán detectados por el receptor.

10111011 1001
3 9

100111011
 1001
 $\overline{6 \quad 0 \quad 0 \quad 1 \quad 1 \quad 0 \quad 1}$
 1001
 61001
 1001

Pseudocodice

\bar{E}

(1001
+ 0001)

100111010
 $\overline{1001}$
 001011
 1001
 001001
 1001
 0000

05 R

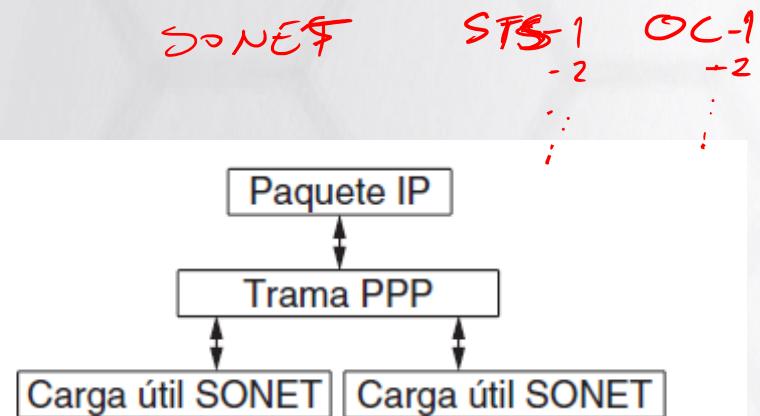
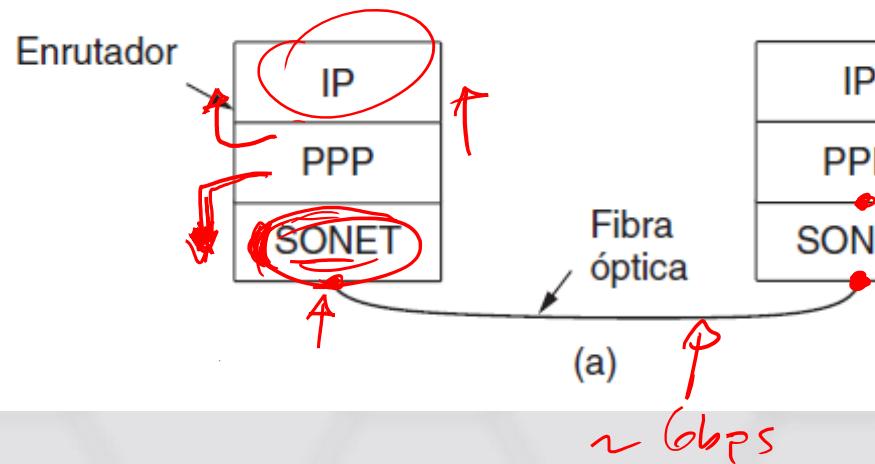
ERRO DETECTADO.

Ejemplos de protocolos (Enlace de datos)

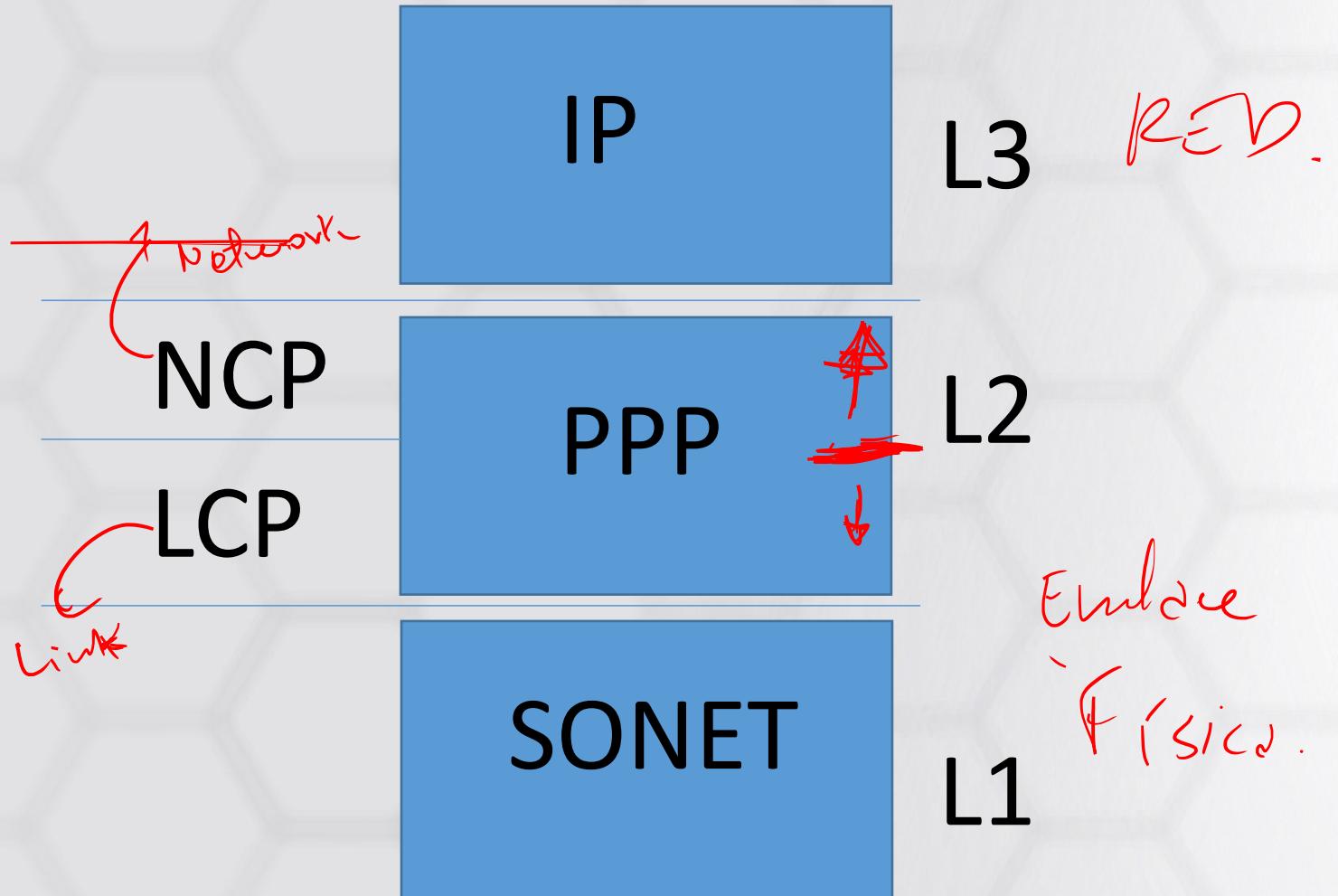
Paquetes sobre SONET

SONET PPP
Point to Point Protocol

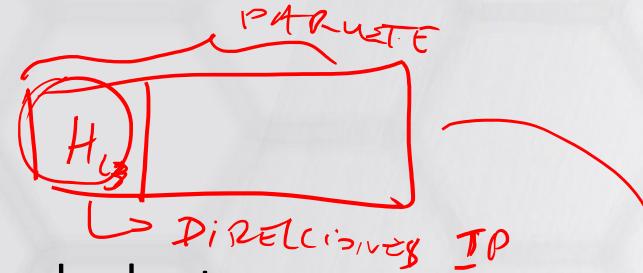
- Para transportar paquetes a través de estos enlaces, se necesita cierto mecanismo de entramado para diferenciar los paquetes ocasionales del flujo de bits continuo en el que se transportan. PPP se ejecuta en enrutadores IP para proveer este mecanismo.



PPP



PPP



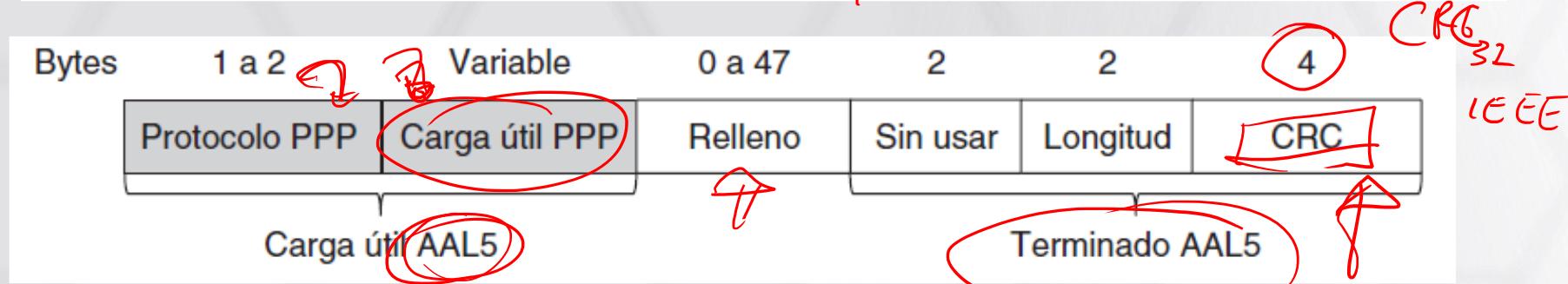
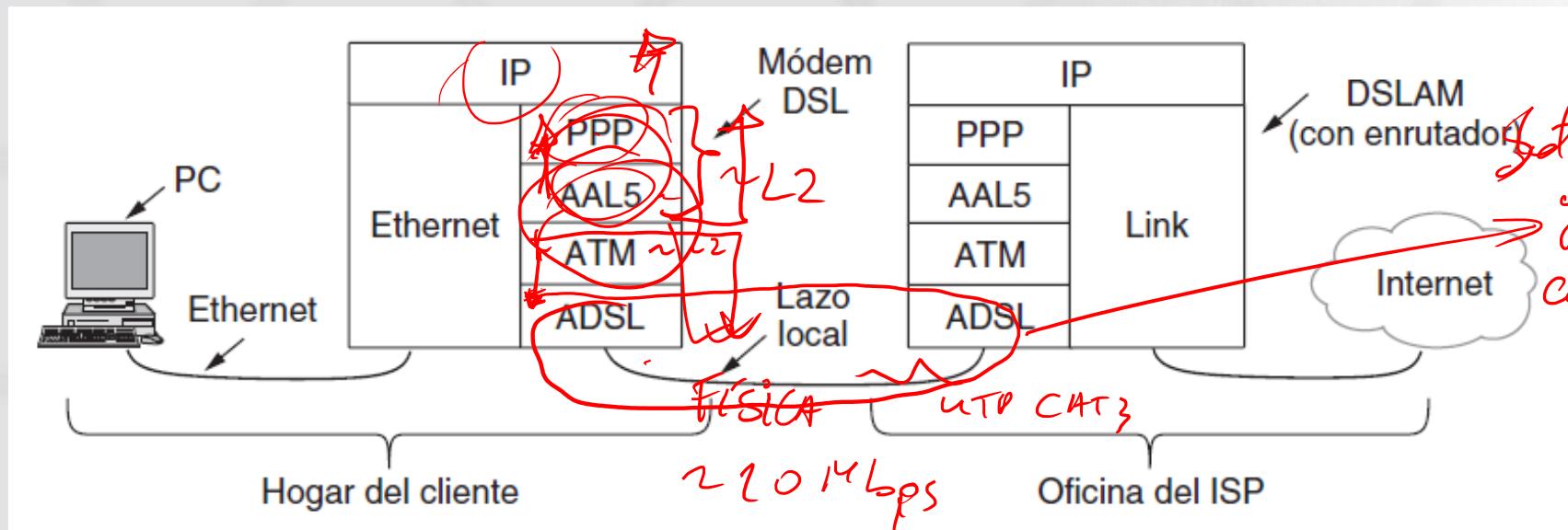
- Utiliza byte bandera y relleno de bytes
- Número entero de bytes (en otros protocolos como HDLC permite fracciones, pues transmite bits y no bytes)
- PPP normalmente se utiliza con un servicio sin conexión (no confirmación de recepción). PAQUETE IP L3

Bytes	1	1	1	1 a 2	Variable	2 a 4	1
	Bandera 01111110	Dirección 11111111	Control 00000011	Protocolo =====	Carga útil 	Suma de verificación	Bandera 01111110

• 7E FF 03 “IP” Polinomio Estándar CRC
Broadcast Trama no numerada

PPP sobre ADSL

~ 24 Mbps.



PPPoA

- PPP over ATM
- ATM (Modo de transferencia asincrónico)
- AAL5 (Capa de adaptación de ATM 5)
- RFC 2364
- Sólo los campos de protocolo y carga útil de PPP se colocan en la carga útil de AAL5.
- Complementa la codificación de ADSL (L1) que usa código Reed-Solomon para corrección y un CRC de 1 byte para la detección

Ejercicios



Ejercicio 37, pág. 219

- ¿Cuál es la sobrecarga mínima para enviar un paquete IP mediante PPP? Tome en cuenta sólo la sobrecarga introducida por el mismo PPP, no la del encabezado IP.

7 bytes

Ejercicio 37, pág. 219

- ¿Cuál es la sobrecarga mínima para enviar un paquete IP mediante PPP? Tome en cuenta sólo la sobrecarga introducida por el mismo PPP, no la del encabezado IP.

