Tema 4:Niveles Superiores

CONTENIDO

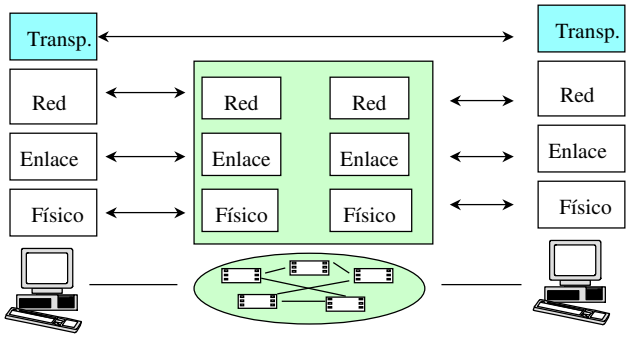
4.1. Nivel de Transporte
4.2. Nivel de Sesión
4.3. Nivel de Presentación

Bibliografía:
* Tanenbaum, “Redes de computadores” Ed. 2ª

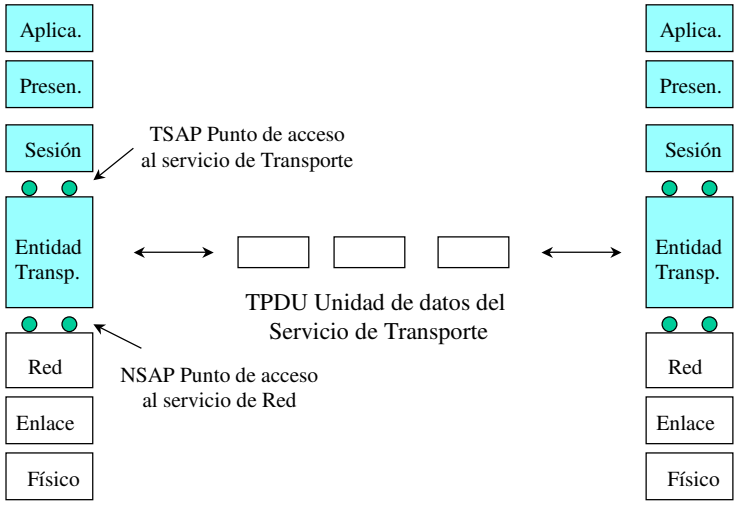
Nivel de Transporte
Introducción.

Objetivo del nivel de transporte:

- Transporte de datos, extremo a extremo, seguro y económico
- Independiente de la red



Nivel de Transporte
Terminología OSI.

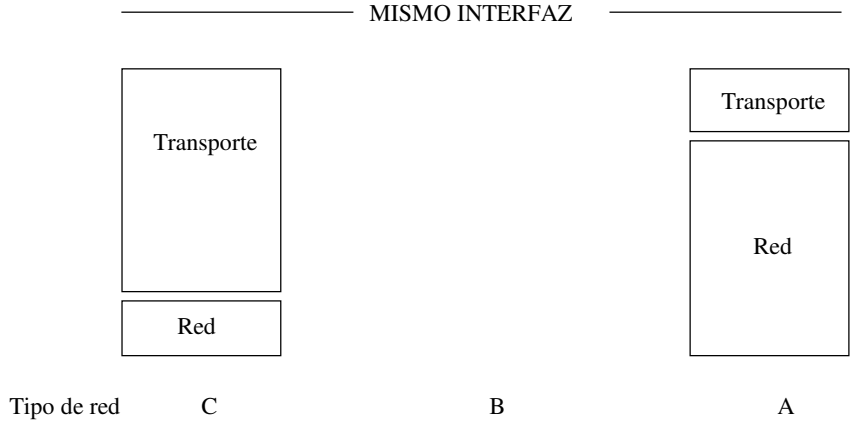


Nivel de Transporte
Tipos de redes.

Para el estudio de los protocolos de transporte, los servicios de red se agrupan en tres categorías:

Tipo de red	Descripción del servicio	Ejemplo
A	Servicio - tasa error muy baja - sin N_RESET	Red de área local
B	Servicio - tasa error baja - con N_RESET	Redes datos publicas (X.25)
C	Servicio inseguro - Perdidas de mensajes - Duplicación de mensajes	WAN Datagramas (Internet)

Nivel de Transporte
Complejidad de transporte.



Nivel de Transporte
Servicios.

Servicios que ofrece transporte al nivel de sesión:

Transporte de datos
- Orientado a conexión
  - Establecimiento, Transferencia y liberación
- Sin conexión

Si los servicios son los mismos que ofrece el nivel de red,

¿ Por que existen niveles de red - transporte ?

- Fiabilidad (Red no está operada por el usuario)
- Mejoras de calidad de servicio (Recuperación de caídas de red)
- Independencia de la red (mismo interfaz con diferentes redes)
- Conjunto normalizado de primitivas
- El destino es diferente (red - maquina, transporte proceso)

Nivel de Transporte
Calidad de servicio.

La calidad de servicio

Conjunto de parámetros destinados a definir diversas cualidades de las conexiones de transporte

- Se especifican en el establecimiento de la conexión
- Normalmente se indican 2 valores: Deseado y mínimo aceptable
- En la negociación de opciones intervienen los dos extremos.

Hay que tener presente que las conexiones con mayor calidad de servicio llevan un incremento de coste (proveedor de servicios)

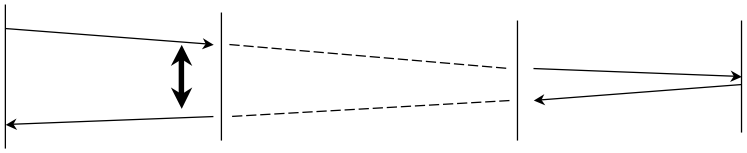
Por ejemplo:

Caudal. Numero de bytes por segundo en una conexión.

Nivel de Transporte
Parámetros de calidad de servicio.

Retardo en el establecimiento de conexión

Tiempo entre la solicitud de conexión de transporte y la confirmación.



Probabilidad de fallo de establecimiento de conexión.

Probabilidad de no establecer la conexión de transporte en el tiempo de retardo permitido.

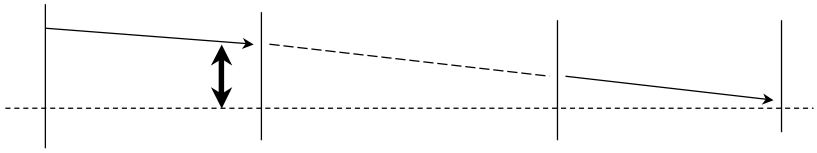
Caudal

Número de bytes / segundo (se mide en los dos sentidos)

Nivel de Transporte
Parámetros de calidad de servicio.

Retardo de transito

Tiempo transcurrido entre el envío de un mensaje y la recepción en el otro extremo



Tasa de error residual

Número de mensajes perdidos o dañados / Total de mensajes

Probabilidad de fallo de transferencia

Número de fallos en caudal, retardo, perdidas / Total de mensajes

Nivel de Transporte
Parámetros de calidad de servicio.

Retardo en liberación de conexión

Tiempo transcurrido entre inicio de liberación y liberación en el otro extremo.

Protección

El usuario puede indicar que la conexión disponga de seguridad ante lecturas o modificaciones.

Prioridad

El usuario puede indicar las conexiones mas importantes. En caso de congestión intentará dar servicio a las conexiones con mayor prioridad.

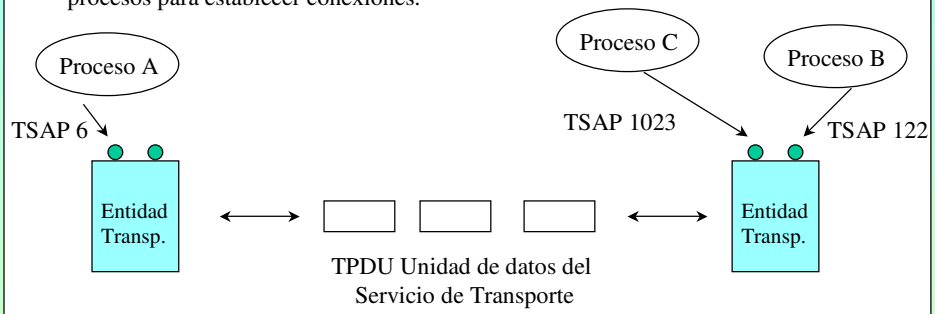
Resistencia

Probabilidad para mantener una conexión ante problemas internos o de congestión

Nivel de Transporte
Administración de conexiones de transporte.

Direccionamiento.

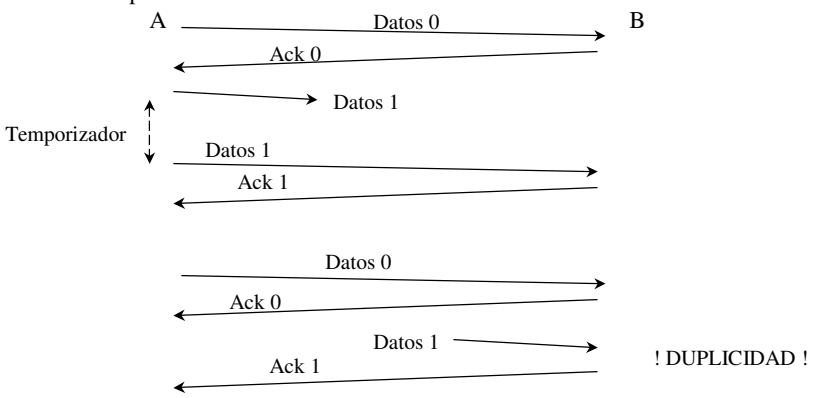
El método básico que se emplea es definir puntos de acceso al servicio de transporte (TSAP, puertos), dotados de dirección, a los que se pueden asociar procesos para establecer conexiones.



Nivel de Transporte
Administración de conexiones de transporte.

Transmisión de TPDU.

En redes tipo **C** puede existir Perdidas, Retrasos y Duplicidad de TPDU
El caso peor son los **DUPLICADOS RETARDADOS**

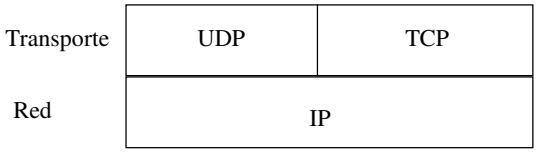


Nivel de Transporte
Transporte en Internet.

En Internet existen dos modalidades de protocolos de transporte:

UDP (User Datagram Protocol)
Protocolo de transporte sin conexión

TCP (Transport Control Protocol)
Protocolo orientado a conexión



Nivel de Transporte
Transporte en Internet.

SOCKET

Primitivas de acceso al servicio de transporte, que el usuario puede integrar en aplicaciones

Pueden utilizar diferentes protocolos, entre ellos TCP/IP

Realizadas de forma específica, no siguen normas de ISO

Basadas en arquitectura Cliente Servidor
La aplicación necesita conocer el papel que va a desempeñar (cliente o servidor) ya que la estructura del sw y primitivas difieren

Permiten comunicaciones orientadas a conexión o sin conexión

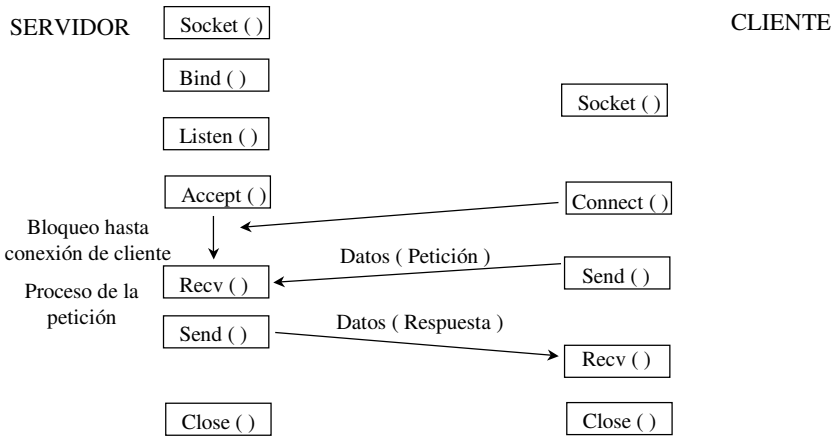
Nivel de Transporte
Transporte en Internet.

Primitivas SOCKET elementales:

Socket	Crea un descriptor de socket.
Close	Cierra socket
Bind	Asocia una dirección local con un socket
Listen	Crea cola de espera para almacenar solicitudes de conexión
Accept	Espera una solicitud de conexión
Connet	Inicia conexión con conector remoto
Shutdown	Finaliza conexión
Send, Write, Sendto	Envía mensaje
Recv, Read, Recvfrom	Recibir mensaje

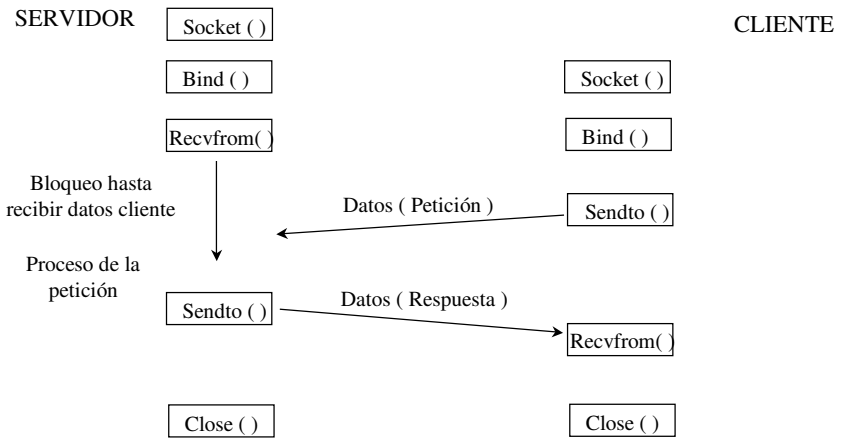
Nivel de Transporte
Transporte en Internet.

Estructura de primitivas en protocolo ORIENTADO A CONEXION



Nivel de Transporte
Transporte en Internet.

Estructura de primitivas en protocolo ORIENTADO A NO CONEXION



Nivel de Presentación.
Contenido.

Introducción
Conversión de datos
- Notación de sintaxis abstracta ASN.1
- Sintaxis de transferencia

Compresión de datos
- Codificación de símbolos equiprobables
- Codificación dependiente de la frecuencia
- Codificación dependiente del contexto

Cifrado de datos
- Cifrado básico
- Norma de cifrado DES
- Criptografía de clave publica

Bibliografía:

* Tanenbaum, “Redes de computadores” Ed. 2ª
* Halsall “Comunicación de datos, redes de computadores y sistemas abiertos” Ed. 4ª

Nivel de Presentación.
Conversión de datos.

Las aplicaciones distribuidas van a permitir el intercambio de información entre **sistemas de diferentes arquitecturas**

Hay que tener en cuenta:

Los sistemas pueden utilizar diferentes representaciones internas de datos
- IBM código EBCDIC
- Otros código ASCII

Aritméticas diferentes
- Complemento a 2
- Complemento a 1

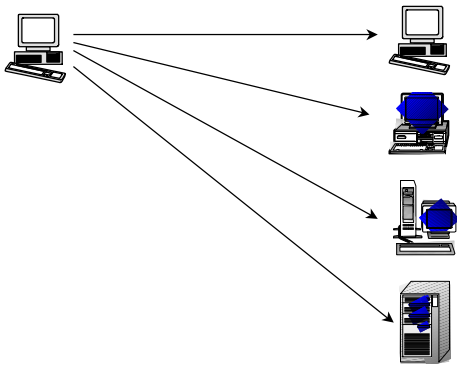
Numeración de la memoria

es necesario realizar una conversión del formato de los datos, para que diferentes sistemas interpreten los datos correctamente

Nivel de Presentación.
Conversión de datos.

Soluciones a la conversión de datos

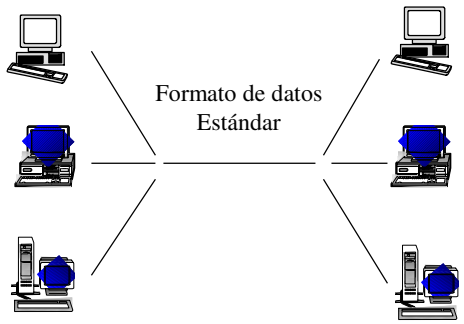
Cada ordenador conoce el formato de datos de los demás
(Es necesaria 1 conversión)



Nivel de Presentación.
Conversión de datos.

Soluciones a la conversión de datos

Utilizar un formato estándar que todos los sistemas conocen
(Son necesarias 2 conversiones)



Nivel de Presentación.
Conversión de datos. Notación de Sintaxis Abstracta ASN.1.

ASN.1 Abstract syntax notation
Normaliza la descripción de estructuras de datos,
con objeto de representar, codificar, transmitir y decodificar estructuras de datos
para evitar los problemas de conversión de datos

Cuando una aplicación quiere enviar una estructura de datos
pasa al nivel de presentación la estructura y su notación ASN.1

Por cada uno de los datos se envía el tipo, longitud y dato en el formato de sintaxis de transferencia

En el otro extremo se localiza la notación y se recompone la estructura
con el formato del sistema destino

Nivel de Presentación.
Cifrado de datos.

Actualmente un amplio grupo de redes (LAN, INTERNET, ….) pueden considerarse como **redes inseguras**, ya que es posible acceder a la información que transporta con cierta facilidad..

La seguridad en el entorno de redes de computadores es un tema que actualmente se encuentra en auge desde diferentes frentes:

- Firewall. Sistemas que restringen accesos a subredes
- Técnicas de acceso al medio en LAN (No broadcast)
- Cifrado de datos
- …….

El cifrado de datos es un conjunto de técnicas que permiten realizar un proceso a la información con anterioridad al envío, con objeto que los datos enviados solamente sean identificables por el destinatario.

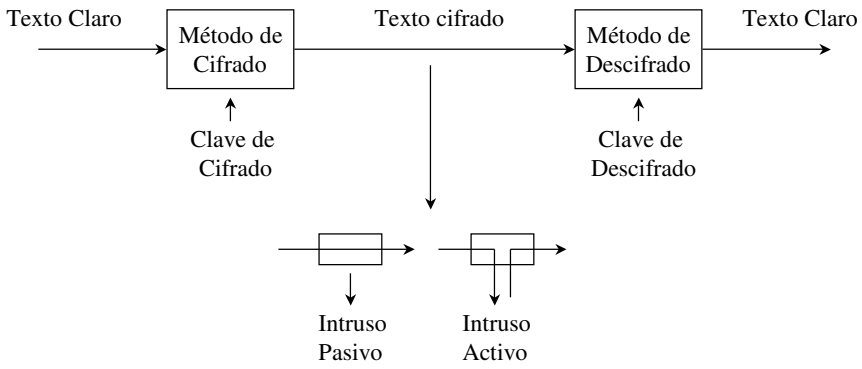
Nivel de Presentación.
Cifrado de datos.

Criptología	Cirptografía	Ciencia de encriptación de textos claros
	Criptoanálisis	Análisis para descifrar textos cifrados

Encriptación de datos	Método	Algoritmo para cifrar textos claros Debe suponerse que los criptoanalistas lo conocen Difícil de mantener en secreto Difícil de cambiar
	Clave	Parámetro del método Selecciona 1 de múltiples cifrados Fácil de cambiar y mantener en secreto

Nivel de Presentación.
Cifrado de datos.

El esquema general del cifrado de datos es el siguiente:



Nivel de Presentación.
Cifrado de datos. Cifrado básico.

Cifradores de sustitución.

Este tipo básico de cifrado sustituye cada letra o grupo de letras por otra letra o grupo de letras.

Sustitución monoalfabética
Consiste en sustituir cada letra por la correspondiente de una tabla.

a b c d e f g h …..
q w e r t y u i …..

Muy fácilmente desencriptable ya que se mantiene la frecuencia de aparición de letras del lenguaje. (p.e, en español la letra mas utilizada en la ‘e’).
Desencriptable mediante
Sustitución de letras de igual frecuencia
Sustitución de digramas, trigramas, palabras, ...

Nivel de Presentación.
Cifrado de datos. Cifrado básico.

Cifradores de sustitución.

Cifradores polialfabéticos

En este tipo de cifrado se dispone de varias tablas de sustitución y una clave

A	a b c d e f g h i j……r s t u v w x y z	Clave CADA
B	b c d e f g h i j……r s t u v w x y z a	
C	c d e f g h i j……r s t u v w x y z a b	
D	d e f g h i j……r s t u v w x y z a b c	
…….		
Z	z a b c d e f g h i j……r s t u v w x y	

La primera letra del texto cifrado se sustituye por la tabla de la primera letra de la clave, la segunda letra por la tabla de la segunda letra de la clave, …

Por ejemplo 'ESTE' se cifra como 'GSWE', y aunque no mantiene la frecuencia de aparición de símbolos del lenguaje, se descifra fácilmente con suficiente texto cifrado

Nivel de Presentación.
Cifrado de datos. Cifrado básico.

Cifradores de transposición.

Este tipo de cifrador reordenan la posición de las letras del texto clara pero no realizan sustitución.

Mantiene la frecuencia de aparición de las letras del lenguaje.

Por ejemplo, un cifrador de transposición columnar clave MEGABUCK (8 columnas orden columnas 7 4 5 1 2 8 3 6):

m	e	g	a	b	u	c	k
7	4	5	1	2	8	3	6
t	e	x	t	o	e	n	c
l	a	r	o	q	u	e	s
e	c	i	f	r	a	r	a

Cifrado: tofoqruereacxricsatleena

Nivel de Presentación.
Cifrado de datos.

La **criptografía moderna** está basada en conceptos de sustitución y transposición

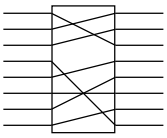
Aunque ahora, debido a la potencia de tratamiento de información, el objetivo es

utilizar algoritmos complejos

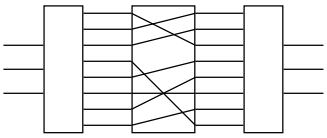
que no puedan ser descifrados aún disponiendo de gran cantidad de texto cifrado.

por ejemplo:

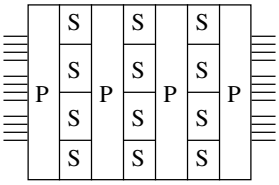
Transposición (Caja P)



Sustitución (Caja S)



Cifrador producto



Nivel de Presentación.
Cifrado de datos. Criptografía de clave publica.

Propone utilizar:

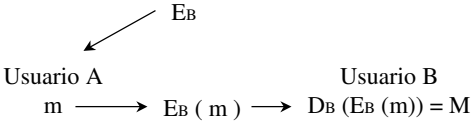
Un algoritmo de cifrado (con clave) E
Un algoritmo de descrifrado (con clave) D

con los requisitos

D (E (m)) = m
A partir de E no se puede deducir D
E no puede descifrarse a partir de E(m)

si se cumplen estos requisitos:

Dar a conocer E públicamente



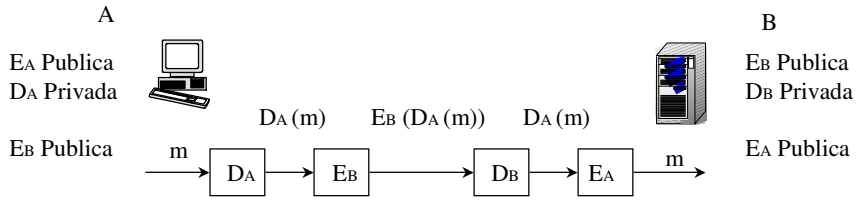
Nivel de Presentación.
Firma Digitales.

Permiten validar un documento ya que el emisor no podrá repudiarlo.

Con clave publica

Es necesario que los algoritmos de cifrado cumplan que

$E(D(m)) = m$ además de **$D(E(m))=m$**



Nivel de Presentación.
Autenticación.

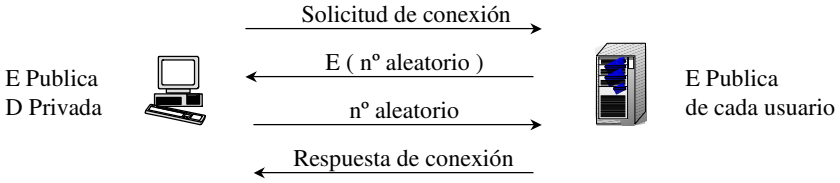
Mecanismo de identificación de la persona que

- Envía un mensaje
- Accede a un sistema

Tradicionalmente se realiza en el momento de efectuar la conexión mediante la inserción de nombre de usuario y una clave de acceso (password).

Mediante clave publica

Cada usuario dispone de una clave publica y otra privada



Nivel de Presentación.
Compresión de datos.

Codificación dependiente de la frecuencia

Si se dispone de un conjunto de símbolos con probabilidades diferentes:

$S_1 P_1 S_2 P_2 \ldots\ldots S_n P_n$

se asignarán
Códigos cortos (menos bits) a los símbolos más probables
códigos largos a los símbolos menos probables

por ejemplo:
A 0,5 B0,1 C 0,25 D 0,15

Con codificación equiprobable A 00 B 01 C 10 D 11

fon entropía $\sum p_i \log_2 1/p_i$ (bits / símbolo) 1,6 bits/símbolo
mediante codificación Huffman A 0 B 110 C 10 D 111

Nivel de Presentación.
Compresión de datos.

Codificación dependiente del contexto.

Los métodos anteriores suponen que la ocurrencia de un símbolo es independiente del anterior.

Si existe una correlación entre símbolos se pueden realizar compresiones eficientes aún cuando exista una distribución plana de símbolos.

Ejemplo:
Comprimir series de símbolos repetidos en nº total y valor del símbolo
Los símbolos han de tomarse dependiendo del contexto donde se encuentren

Imagen (pixel de 16 bits)
compresión nº de pixel iguales - valor pixel (16 bits)