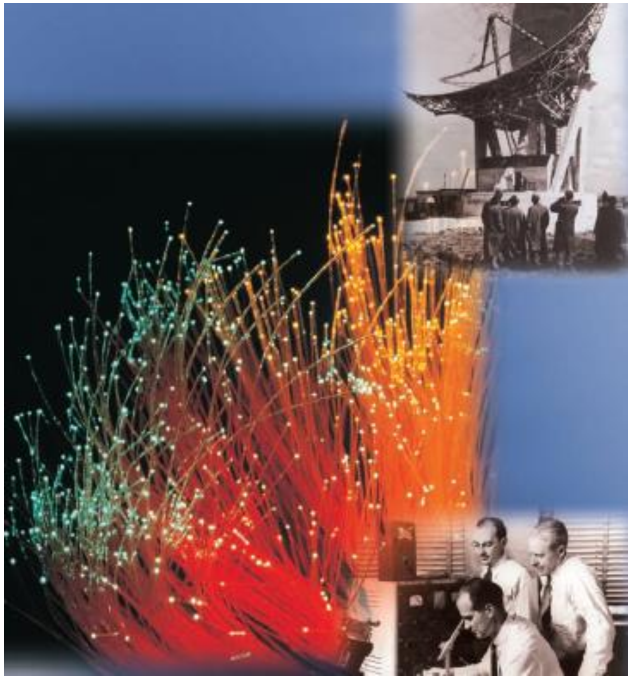
¡Bienvenidos!

Teoría de las Comunicaciones (a.k.a. Redes)

Claudio Enrique Righetti

Segundo Cuatrimestre de 2017

Departamento de Computación
Facultad de Ciencias Exactas y Naturales
Universidad de Buenos Aires
Argentina



Introducción

Fundamentos

Imagen de la tapa del libro **A Brief History of Communications** IEEE Communications Society - A Fifty Year Foundation for the Future - 1952-2002

"Cuando se proclamó que la Biblioteca abarcaba todos los libros, la primera impresión fue de extravagante felicidad. Todos los hombres se sintieron señores de un tesoro intacto y secreto. No había problema personal o mundial cuya elocuente solución no existiera: en algún hexágono."

Jorge Luis Borges, « *La Biblioteca de Babel* »

Agenda (Clase 15-Agosto-2017)

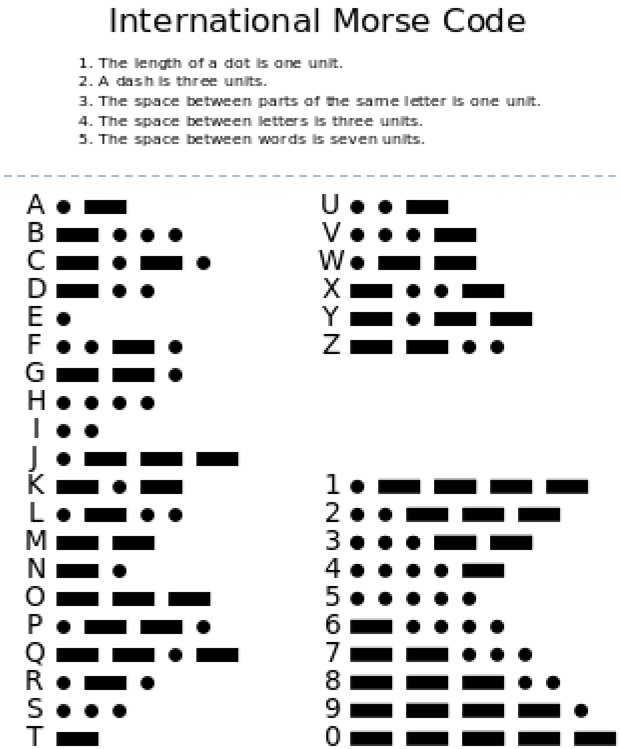
- Presentación
- La red eléctrica, la red telefónica.
- Los grandes paradigmas: Conmutación de Circuitos vs. Conmutación de Paquetes
- Multiplexación: en el Tiempo , Frecuencia y "Estadística"
- Arquitectura de Redes: Modelo de Referencia OSI-ISO – TCP/IP
- Algunas palabras claves …

Bibliografía

- Andrew S. Tanenbaum and David J. Wetherall. 2010. *Computer Networks* (5th ed.). Prentice Hall Press, Upper Saddle River, NJ, USA
  - Los capítulos 1 (Introducción) y 2 (Nivel Físico)
- Larry L. Peterson and Bruce S. Davie, 2011. *Computer Networks, Fifth Edition: A Systems Approach* (5th ed.). Morgan Kaufmann Publishers Inc., San Francisco, CA, USA.
  - La mayor parte de la materia
- Abramson Norman Information, 1963. Theory and Coding. First edition McGraw Hill, USA.
  - Libro es sobre teoría de la Información y codificación
  - Sus primeros capítulos son el texto oficial de la materia para estos temas.
  - Versión en español: "Teoría de la Información y Codificación", Paraninfo, 1986

Y fue el telégrafo …

- Samuel Morse y su Código



- Y llegamos al teléfono

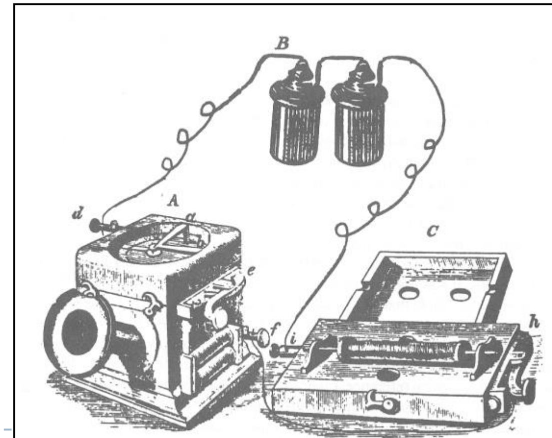
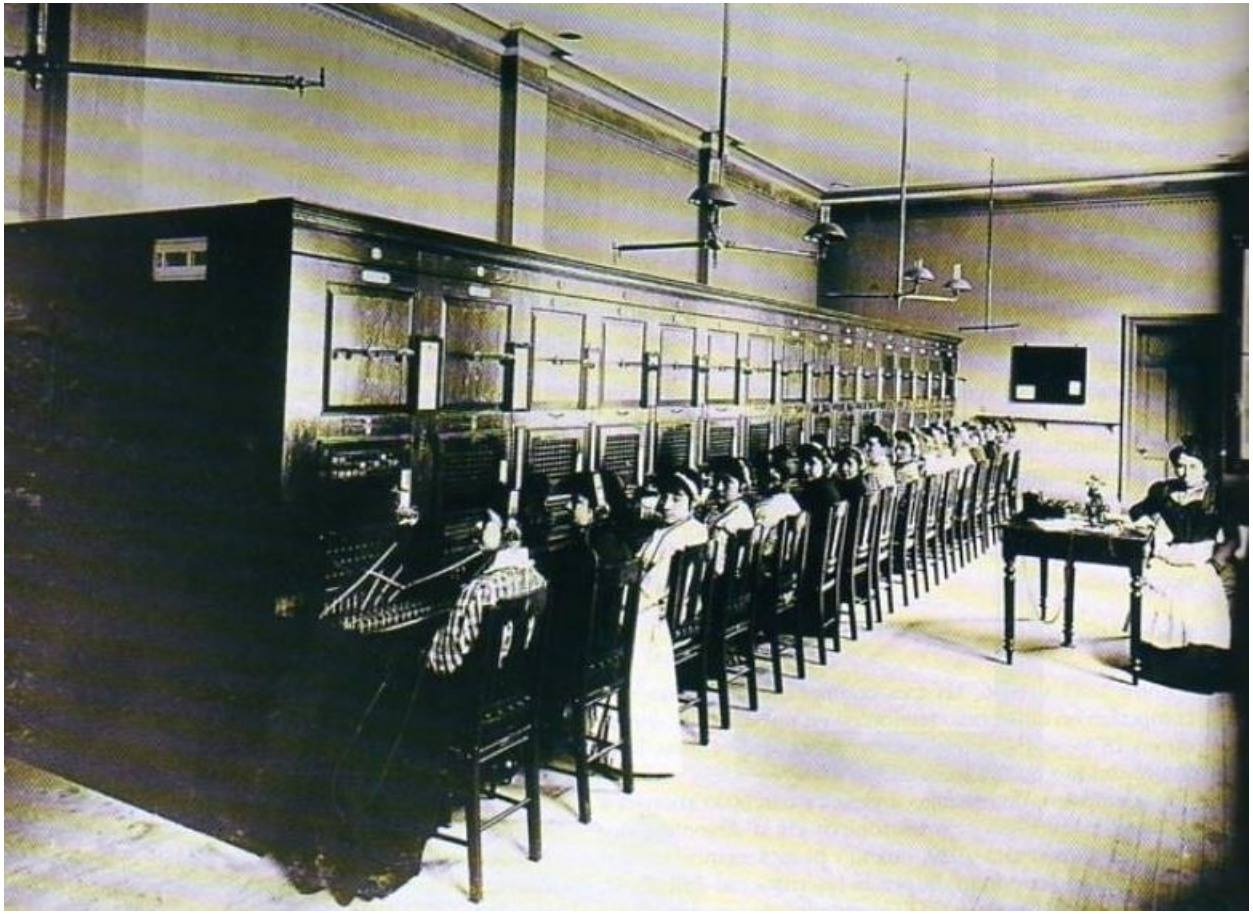


Figure 1.1 Back to the future: the first integrated voice/data communication system.

Central de conmutación de circuitos



Inicios de la conmutación de paquetes: la “semilla” de Internet

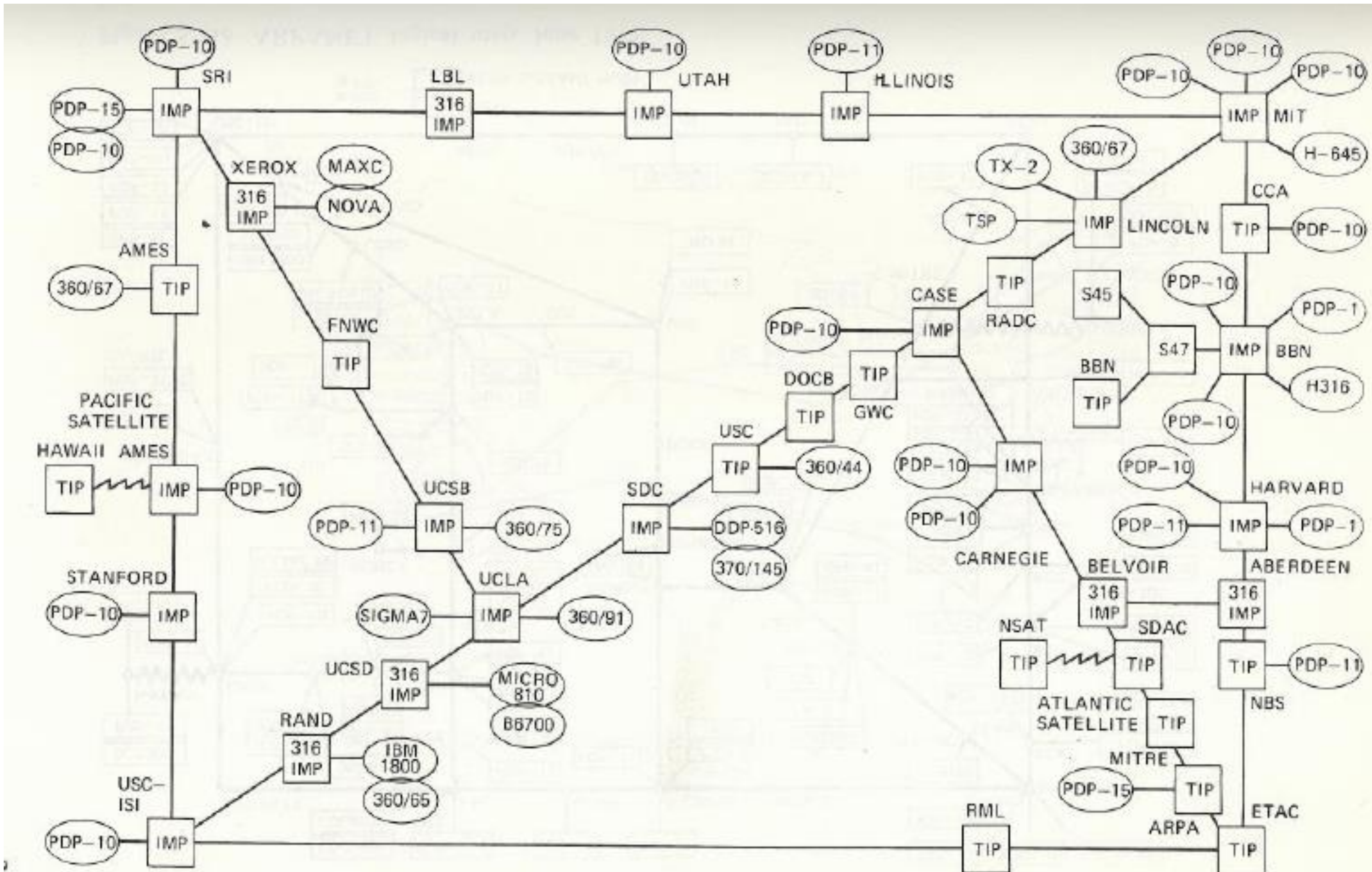
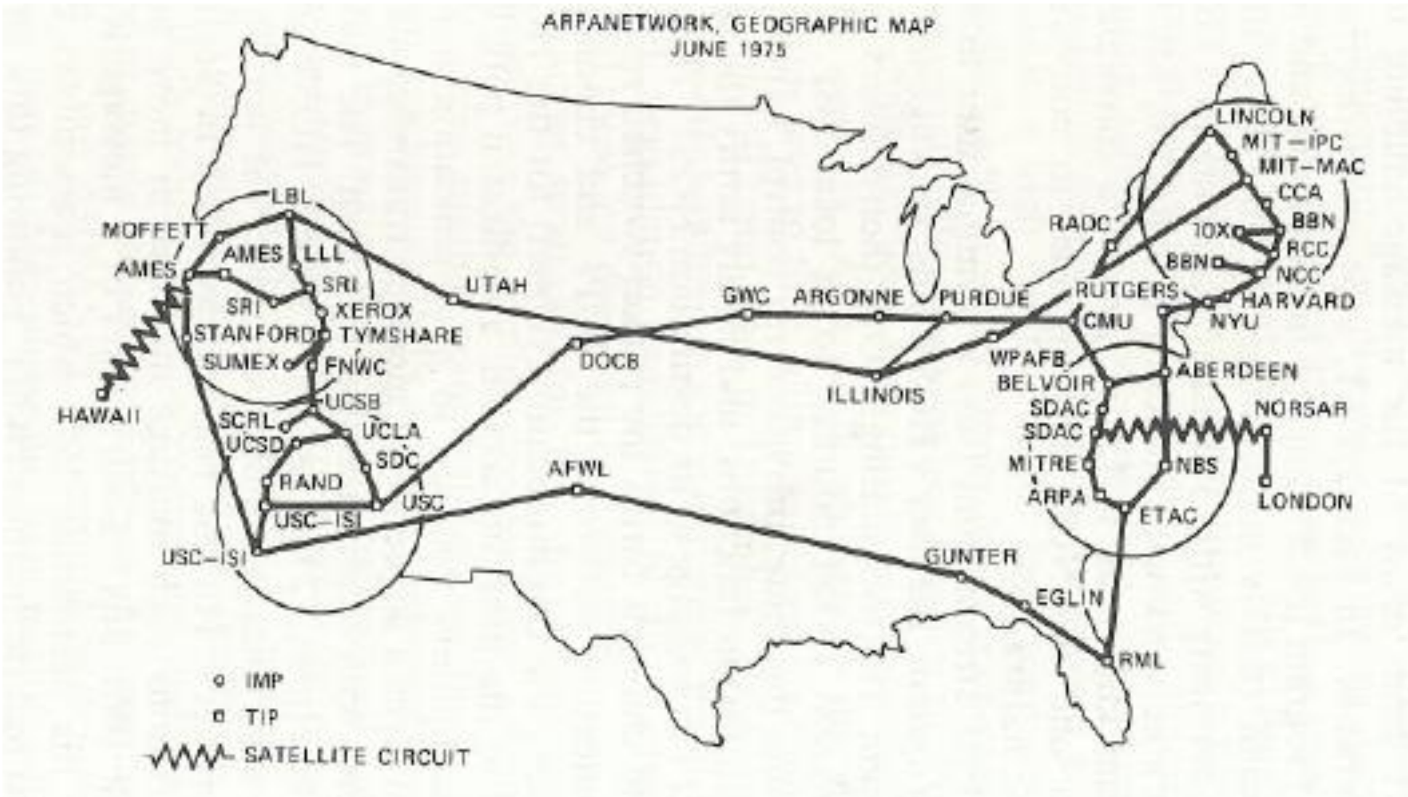


Figure 5.21 (*a*) ARPANET, logical map, August 1973.

The **Advanced Research Projects Agency Network (ARPANET)** was an early packet switching network and the first network to implement the protocol suite TCP/IP.

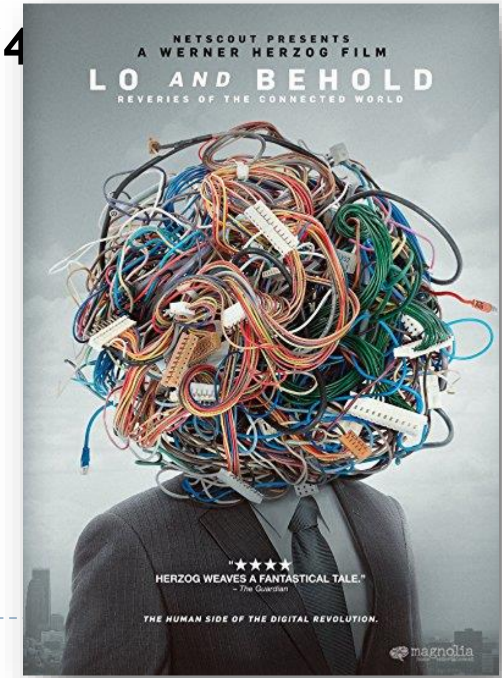
Inicios de la conmutación de paquetes: la “semilla” de Internet



Algunos Trabajos fundacionales

- **Kleinrock**, L. "**Models for Computer Networks**", Conference Record, *IEEE International Conference on Communications*, Boulder, Colorado, pp. 21-9 to 21-16, June **1969**

- **Kleinrock**, L. and W. Naylor, "**On Measured Behavior of the ARPA Network**", AFIPS Conference *Proceedings, Vol. 43, National Computer Conference*, Chicago, Illinois, AFIPS Press, Montvale, New Jersey, pp. 767-780, May **1974**
- Recomendado: **Leonard Kleinrock** contando el inicio de Internet
  - **Documental "LO and BEHOLD" (2016)** acerca de Internet, del gran cineasta Werner Herzog.
  - http://www.loandbehold-film.com/trailer
  - **Internet comenzó con una falla el 29 de Oct. de 1969 en UCLA: "LO" no llegó a ser "LOGIN"**



MODELS FOR COMPUTER NETWORKS†

Leonard Kleinrock
Associate Professor
School of Engineering and Applied Science
University of California at Los Angeles
Los Angeles, California 90024

Abstract

The important task of predicting performance of computer networks is considered. In this initial approach, both mathematical and simulation models are described, and the results obtained are compared so as to identify their differences. Suggestions are made with regard to creating more sophisticated mathematical models which will predict more accurately the behavior of computer networks. The driving force which motivates this analysis is the experimental computer network currently being implemented through the efforts of the Advanced Research Projects Agency in the Department of Defense.

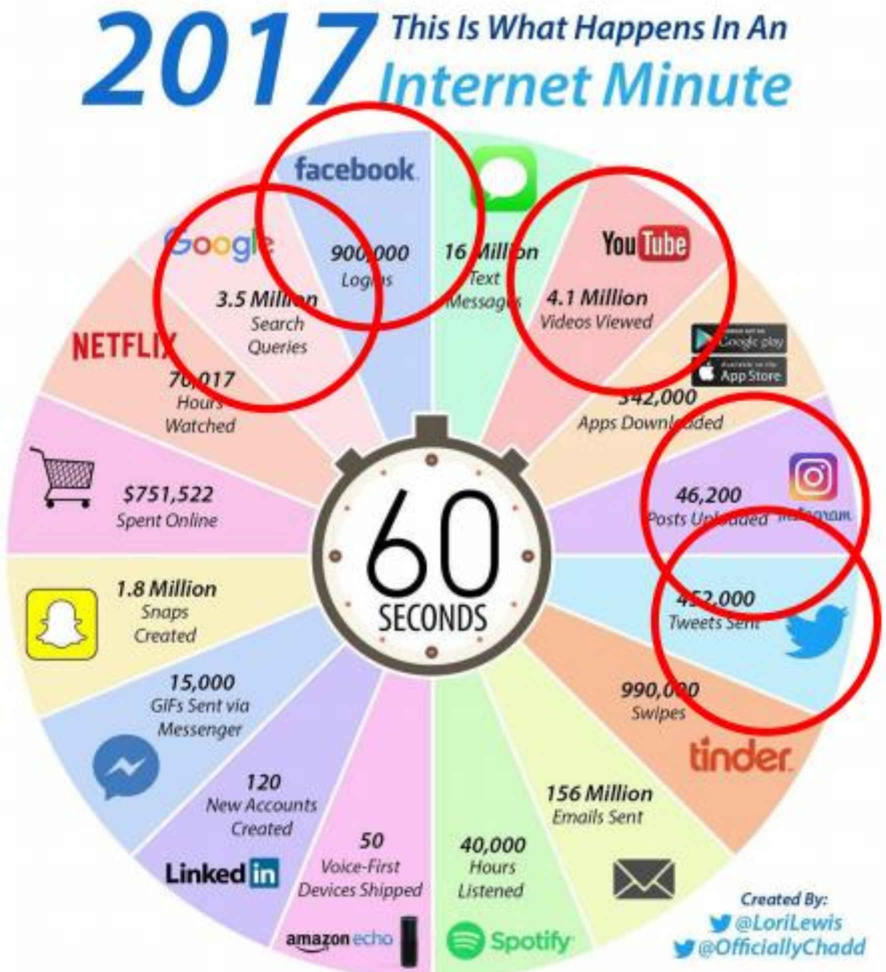
I. Introduction

!!!!! Computer networks are not new. SAGE[1] was one of the first as was the American Airlines reservation system.[2] Numerous military nets have been created and, of course, there is the huge electronically-switched telephone system. Recently CDC announced their nationwide com-

continental United States. The computers located at each of the nodes are highly incompatible (e.g. S.D.S. 940, DEC PDP-10, IBM 360/67, UNIVAC 1108, GE 635, ILLIAC 4, TX-2, etc.), and one of the major challenges is to design a network in which this assortment of varied hardware and software systems can communicate and cooperate with each other. The principle motivation for creating this network is to provide to each of the computer research centers those special resources which have been created at the other centers.. For example, Stanford Research Institute will provide the role of network librarian and will offer its sophisticated text editing capability for massaging this vast data base; University of Illinois will allow access to the extremely high parallel processing speeds of its ILLIAC 4; University of Utah will serve as a major graphics center for picture processing; University of California at Los Angeles will process network measurement data and compare these to simulation and analytically predicted results.

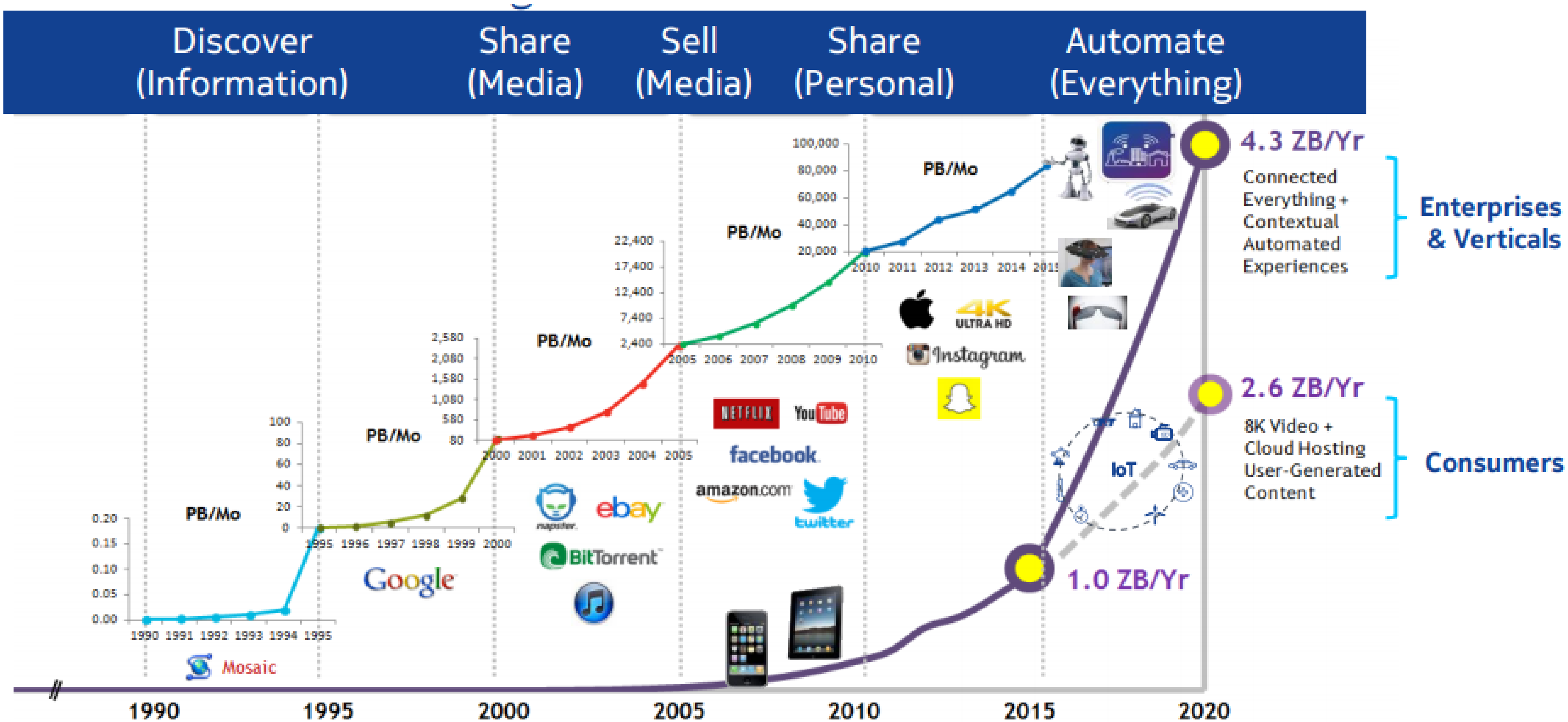
References

1. R.R. Everett, C.A. Zraket, and H.D. Benington," SAGE: A Data Processing System for Air Defense," EJCC, pp. 148-155, 1957.
2. J. Evans, "Experience Gained from the American Airlines SABRE System Control Program," Proc. ACM National Meeting August 1967, pp. 77-83.



2017 This Is What Happens In An Internet Minute
facebook
900,000 Logins
16 Million Text Messages
YouTube
4.1 Million Videos Viewed
342,000 Apps Downloaded
46,200 Posts Uploaded
452,000 Tweets Sent
990,000 Swipes
tinder
156 Million Emails Sent
40,000 Hours Listened
Spotify
50 Voice-First Devices Shipped
amazon echo
120 New Accounts Created
LinkedIn
15,000 GIFs Sent via Messenger
1.8 Million Snaps Created
$751,522 Spent Online
NETFLIX
70,017 Hours Watched
Google
3.5 Million Search Queries
60 SECONDS
Created By:
@LoriLewis
@OfficiallyChadd

Evolución de la demanda



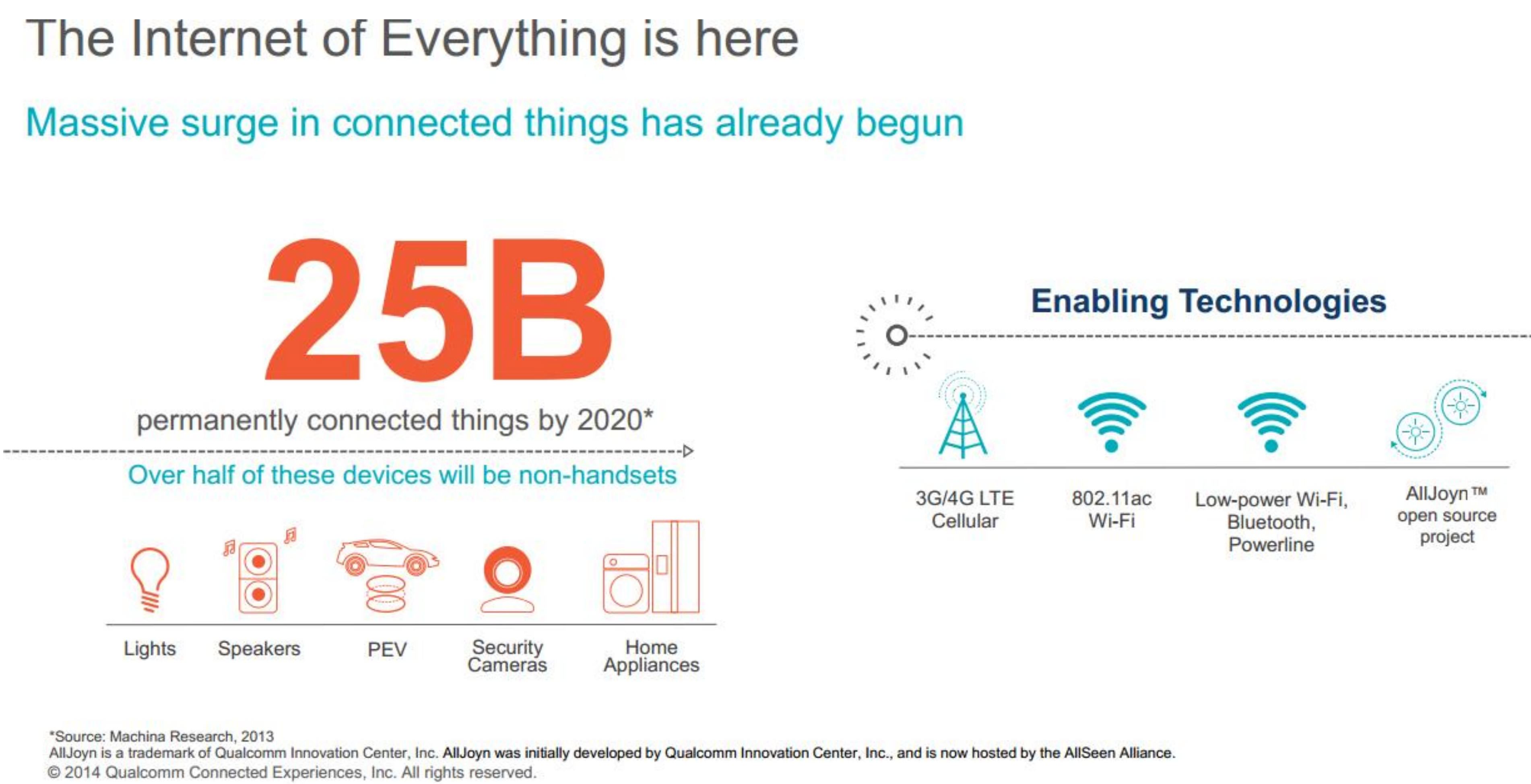
Fuente : NOKIA

Lo que se viene…

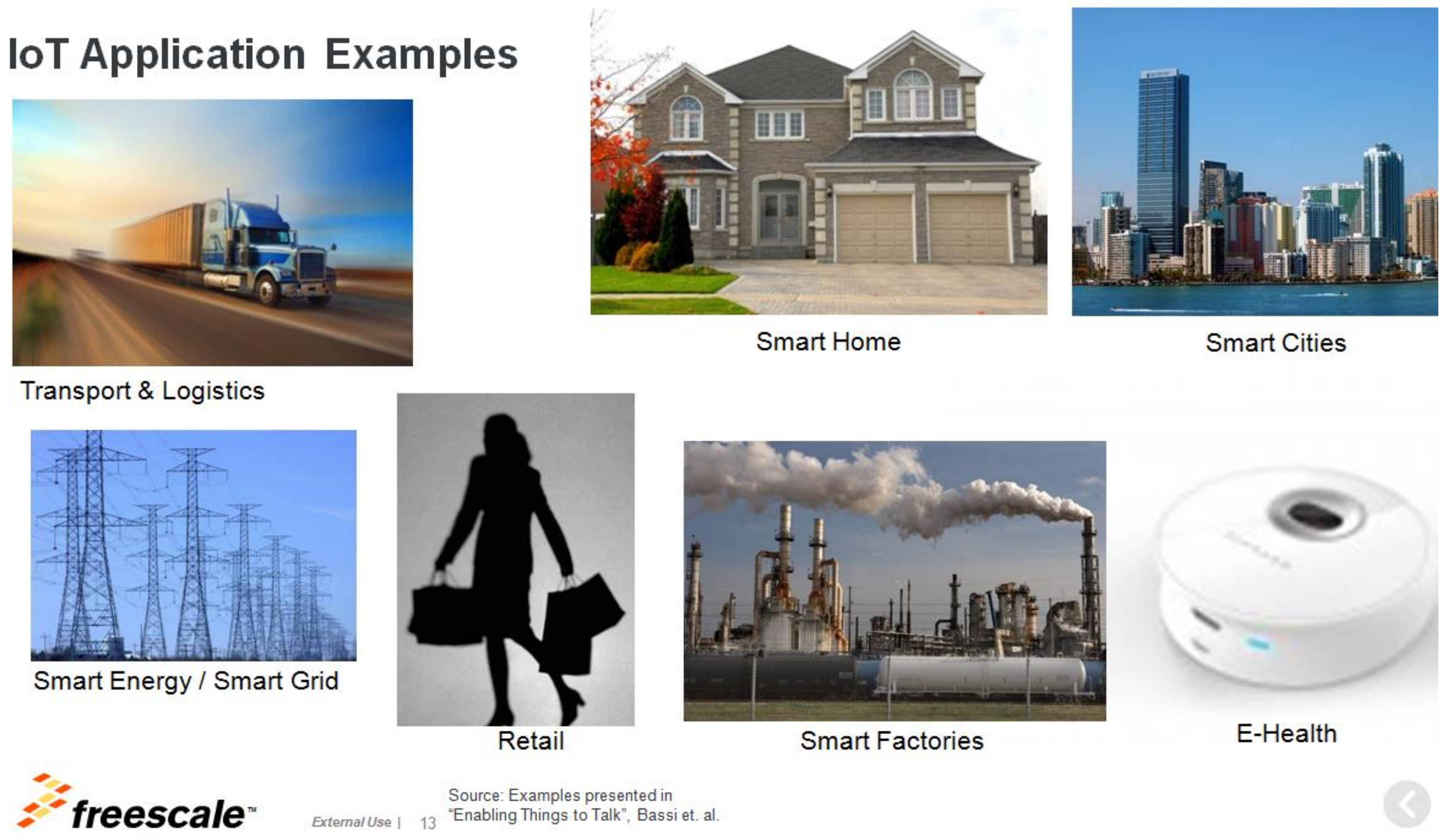
- Comunicaciones cuánticas
- NFV/SDN/CRN
- Banda Ancha > 1Gbps , bajar la latencia
- 5 G
- "Internet de las Cosas"

"La mayoría de las comunicaciones telefónicas se realizan actualmente mediante celulares, y las redes de datos y voz aun tienen infraestructuras diferentes. Pero es probable que a finales del 2020 termine esta convergencia y se unifique una red global basada en Internet, y todas las llamadas viajarán por la red. Entonces, desde cualquier dispositivo conectado podremos realizar, por ejemplo, videollamadas en forma masiva. Las estimaciones son que habrá unos 50.000 millones de dispositivos en red, que nos brindaran información sobre condiciones de seguridad de nuestro hogar, parámetros vitales de nuestros ancianos, historia médica, entre otros aspectos"
http://web.clarin.com/sociedad/evolucion-mira-Internet_0_892710831.html

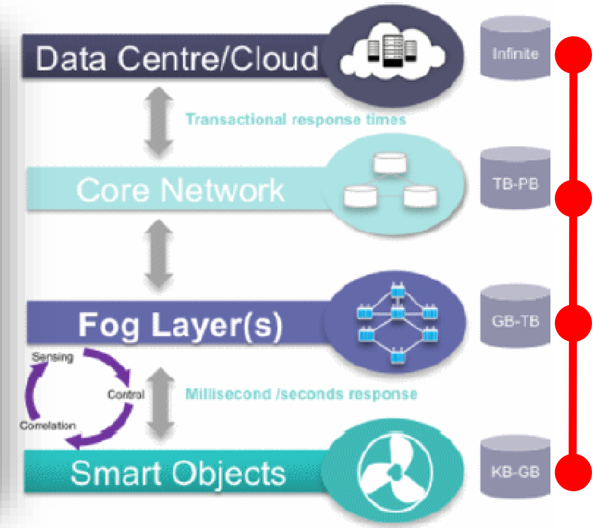
Lo que se viene… IoE

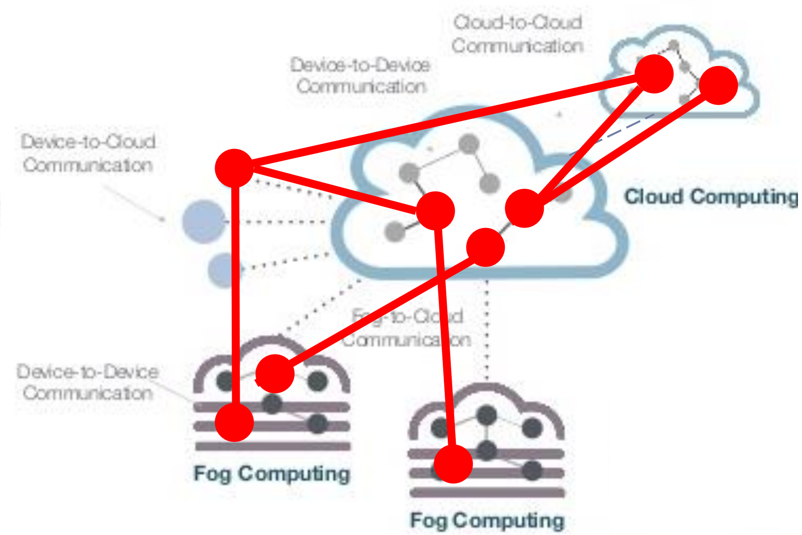


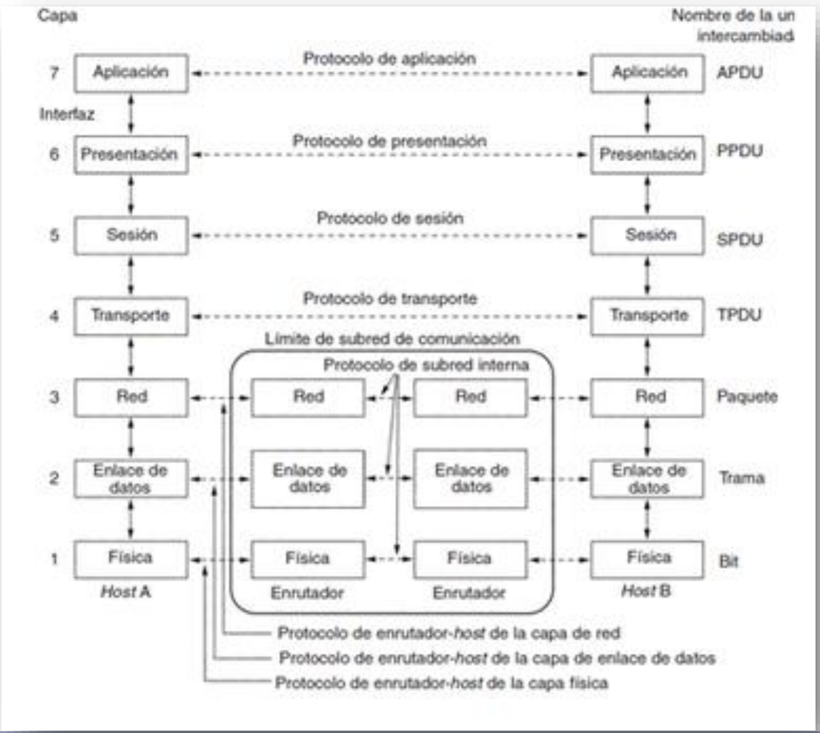
Lo que se viene… IoE



IoT en Ciudades Inteligentes







Arquitectura de Redes

Fundamentos

Figura del libro de Tanenbaum

Múltiples Redes Globales

UUCP	g!d.!!u	g!d.!!u	g!h.mailnet!!u
JUNET	u@d.I.arpa	u@d.I.arpa	u%h.mailnet@mit-multics.arpa

Domains: From / To:	U: uk JANET	E: cdn, dfn, etc. EAN	COSAC
ARPA Internet	u%d.U@cs.ucl.ac.uk	u%d.E%ubc.csnet@relay.cs.net	h/u%france.csnet@relay.cs.net
CSNET Phonenet	u%d.U@cs.ucl.ac.uk	u%d.E@ubc.csnet	h/u@france.csnet
MAILNET	?	u%d.E@ubc.mailnet	?
JANET	u@U.d	u@d.U	?
EAN	u@d.U	u@d.E	h/u@france.csnet
COSAC	?	?	h/u
BITNET	u%d.U@ac.uk	u@d.E	h/u@france.csnet
ACSNET	u%d.U@munnari.oz	u%d.E@munnari.oz	h/u%france.csnet@munnari.oz
UUCP	g!cs.ucl.ac.uk!d.U!u	g!d.E!u	?
JUNET	u@d.U.janet	u%d.E@ubc.csnet	h/u@france.csnet

Domains: From / To:	R: A registry Xerox Internet	DEC's Easynet	IBM's VNET
ARPA Internet	u.R@xerox.com	u%h.dec@decwrl.dec.com	u%h@ibm.com
CSNET Phonenet	u.R@xerox.com	u%h.dec@decwrl.dec.com	u%h@ibm.com
MAILNET	?	?	?
JANET	?	?	?
EAN	u.R@xerox.com	u%h.dec@decwrl.dec.com	u%h@ibm.com
COSAC	?	?	?
BITNET	u.R@xerox.com	u%h.dec.com@decwrl.dec.com	u@vnet
ACSNET	u.R%xerox.com@munnari.oz	u%h.dec.com@munnari.oz	u%h%ibm.com@munnari.oz
UUCP	parcvax!u.R	decwrl!h.dec.com!u	g!ibm.com!u%h
JUNET	u.R@xerox.com.arpa	u%h.dec@decwrl.dec.com.arpa	u%h@ibm.com.arpa

Domains: From / To:	BITNET	A: oz.au ACSNET	UUCP	J: junet JUNET
ARPA Internet	u%h.bitnet@wiscvm.wisc.edu	u@d.A	u%h.uucp@g	u%d.J%utokyo-relay@relay.cs.net
CSNET Phonenet	u%h.bitnet@relay.cs.net	u@d.A	u%h.uucp@g	u%d.J@utokyo-relay
MAILNET	?	u%d.A%g@mit-multics	?	u%d.J%csnet-relay@mit-multics
JANET	?	u%d.oz@uk.ac.ukc	?	u%d.J@uk.ac.ukc
EAN	u@h.bitnet	u@d.A	u@h.uucp	u%d.J@relay.cs.net
COSAC	adi/u%h.bitnet@relay.cs.net	?	adi/u%h.uucp	adi/u%h.J@relay.cs.net
BITNET	u@h	u%d.A@g	h1!h2!h!u@psuvax1	u%d.J@csnet-relay.csnet
ACSNET	u%h.bitnet@munnari.oz	u@d.A	u%h.uucp@munnari.oz	u%d.J@munnari.oz
UUCP	psuvax1!h.bitnet!u	seismo!munnari!d.A!u	h1!h2!h!u	g!d.J!u
JUNET	u@h.bitnet	u@d.A	u@h.uucp	u@d.J

Notes: From UUCP to CDNnet ubc-ean is a gateway; from EUnet to the European EAN networks there is one gateway per country; there is more than one gateway between BITNET and UUCP; UUCP, EUnet, and SDN are similarly addressed, so only one of them is listed here.
Abbreviations: u: user; h: host; g: gateway (unnamed here); d: domain.
Omissions: From company networks, with commercial networks, with the ARPA Intenet.

[QH86] John S. Quarterman and Josiah C. Hoskins. 1986. Notable computer networks. *Commun. ACM* 29, 10 (October 1986), 932-971.

Como escribíamos una dirección …

steve@cs.ucl.ac.uk	Via ARPA Internet
. . . !ucl-cs!steve	Via UUCP
steve@uk.ac.ucl.cs	Via JANET
gb/bt/des/steve(ucl/cs)	X.400, GIPSI (of INRIA) UIP
/C=GB/ADMD=BT/PRMD=DES/O=UCL/ OU=CS/S=Kille/	X.400, RFC987 UIP
⟨C=gb;A=bt;P=des;O=ucl;S=steve;OU=cs⟩	X.400, another UIP
steve!ucl!cs&des%bt&gb	X.400, DFN UIP
steve!ucl!cs#des&bt.gb	X.400, EARN/X.400 gateway UIP
steve@cs.ucl.des.bt.gb	EAN, RFC822 UIP and domain order
/C=/ADMD=/PRMD=UK/DD.=cs.ucl.ac/ DD.=steve/	EAN, X.400 encoding, RFC987 UIP

FIGURE 1. Sample Addresses for Different Networks

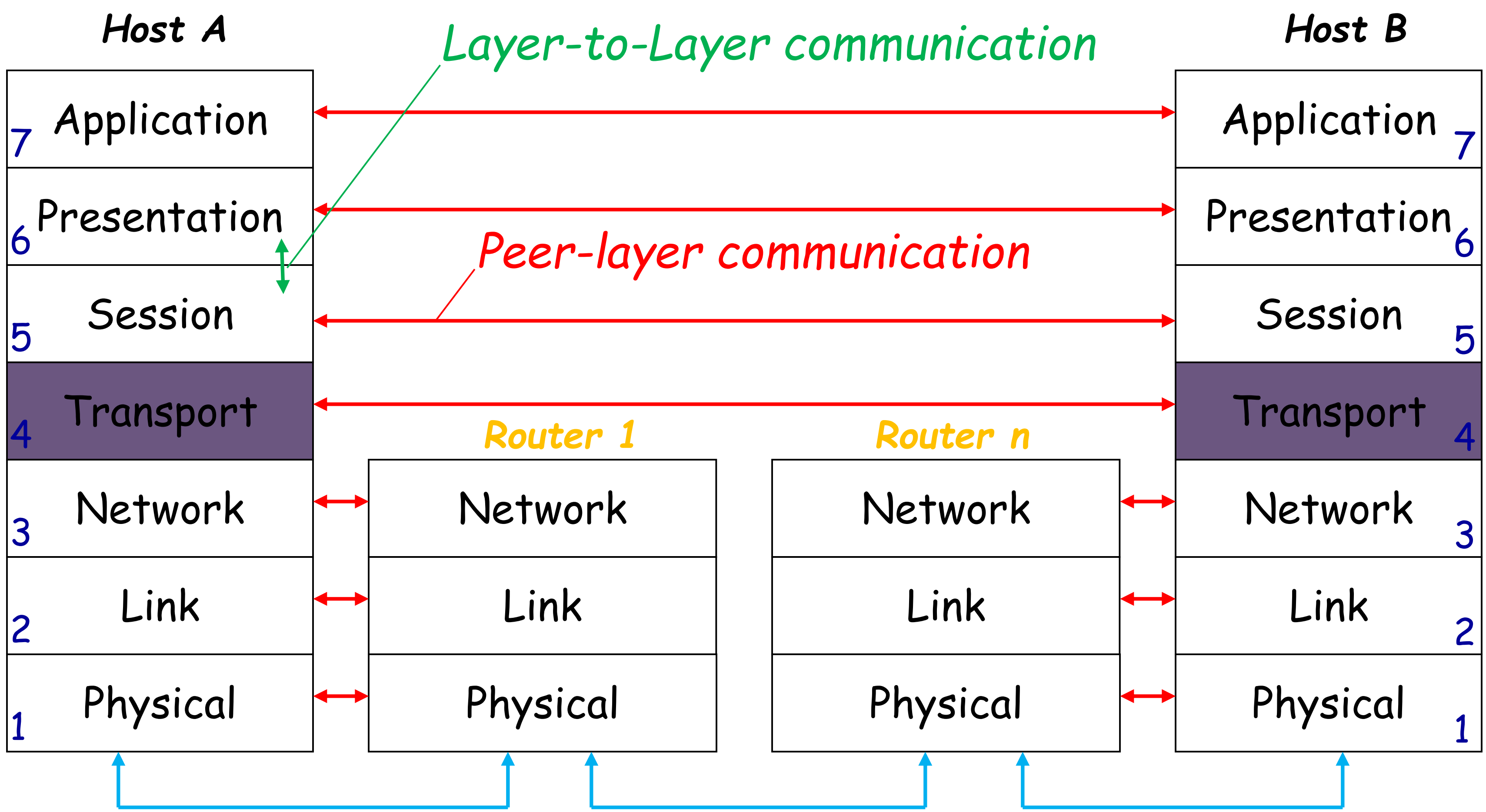
[QH86] John S. Quarterman and Josiah C. Hoskins. 1986. Notable computer networks. *Commun. ACM* 29, 10 (October 1986), 932-971.

Múltiples Redes Globales

- BITNET, XEROX, DECNET ...
- ARPANET, CSNET, MILNET, UUCP ..
  - Esta era la situación a mediados de los 80
    - Quaterman realiza un survey de las principales redes Globales de la época [QH86]
- Una arquitectura única de Red (OSI –ISO)?
- **Mayo 1983:** ISO publica "*ISO 7498: The Basic Reference Model for Open Systems Interconnection*" as an international standard.

[QH86] John S. Quarterman and Josiah C. Hoskins. 1986. Notable computer networks. *Commun. ACM* 29, 10 (October 1986), 932-971.

Modelo OSI



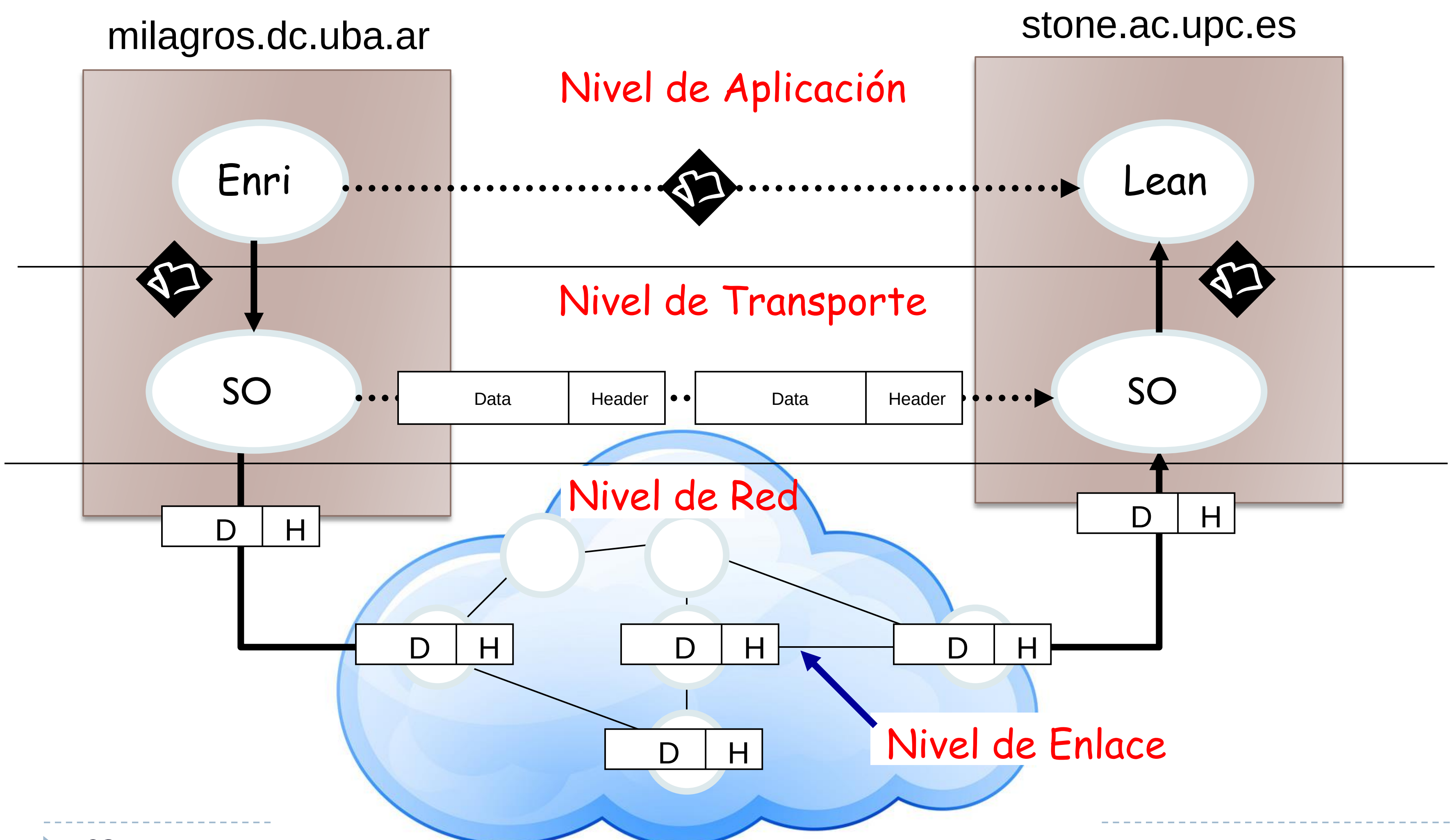
Hubbert Zimmermann, 1980
http://www.cs.cmu.edu/~srini/15-744/F02/readings/Zim80.pdf


IEEE TRANSACTIONS ON COMMUNICATIONS, VOL. COM-28, NO. 4, APRIL 1980 425

OSI Reference Model—The ISO Model of Architecture for Open Systems Interconnection

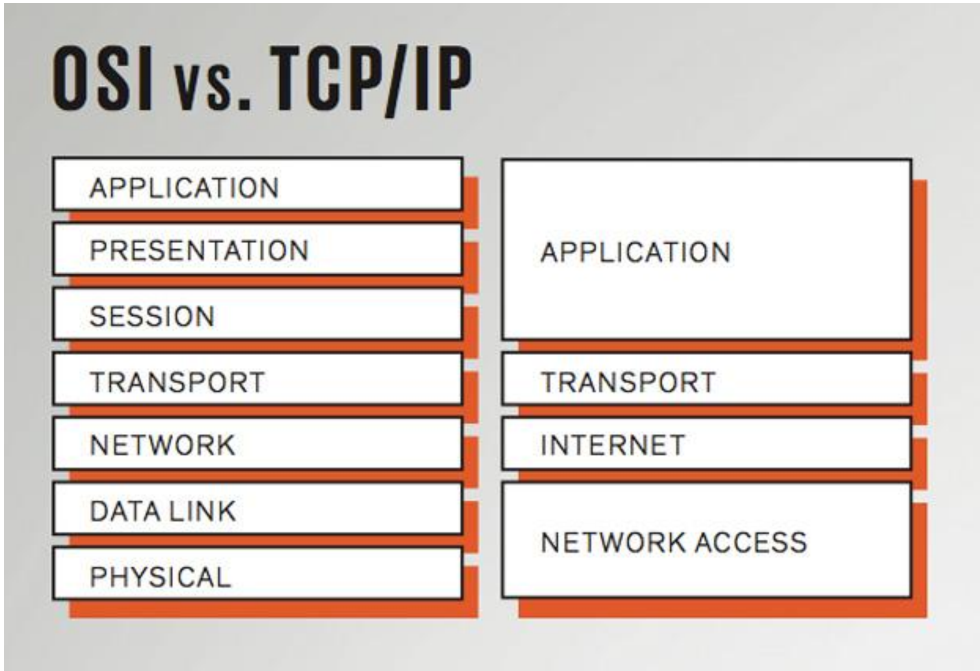
HUBERT ZIMMERMANN

Nivel Transporte: "End to End"



Como se impuso TCP/IP a OSI ?

- Una visión de las causas la pueden encontrar en:
- http://spectrum.ieee.org/computing/networks/osi-the-internet-that-wasnt



La historia la escriben …

- http://www.comsoc.org/files/Publications/Magazines/ci/hist-comm/2010-aug.pdf
- http://www.comsoc.org/files/Publications/Magazines/ci/hist-comm/2012-may.pdf
- http://www.comsoc.org/files/Publications/Magazines/ci/hist-comm/2009-feb.pdf
- http://www.internetsociety.org/internet/what-internet/history-internet/brief-history-internet
- http://es.wikipedia.org/wiki/Historia_de_Internet

Mito urbano: "Internet es producto de la guerra fría … "

Agenda (Parte 2)

- Modelo de Sistema de Comunicaciones
- Mundo Analógico y Digital
- Fundamentos de las señales
- En el dominio de la frecuencia
  - Fourier – Ancho de Banda
- Introducción a la Teoría de la Información

Nivel Físico

Parte 1 - Fundamentos

http://www.sciencephoto.com/media/225137/view

Sistema de Comunicaciones

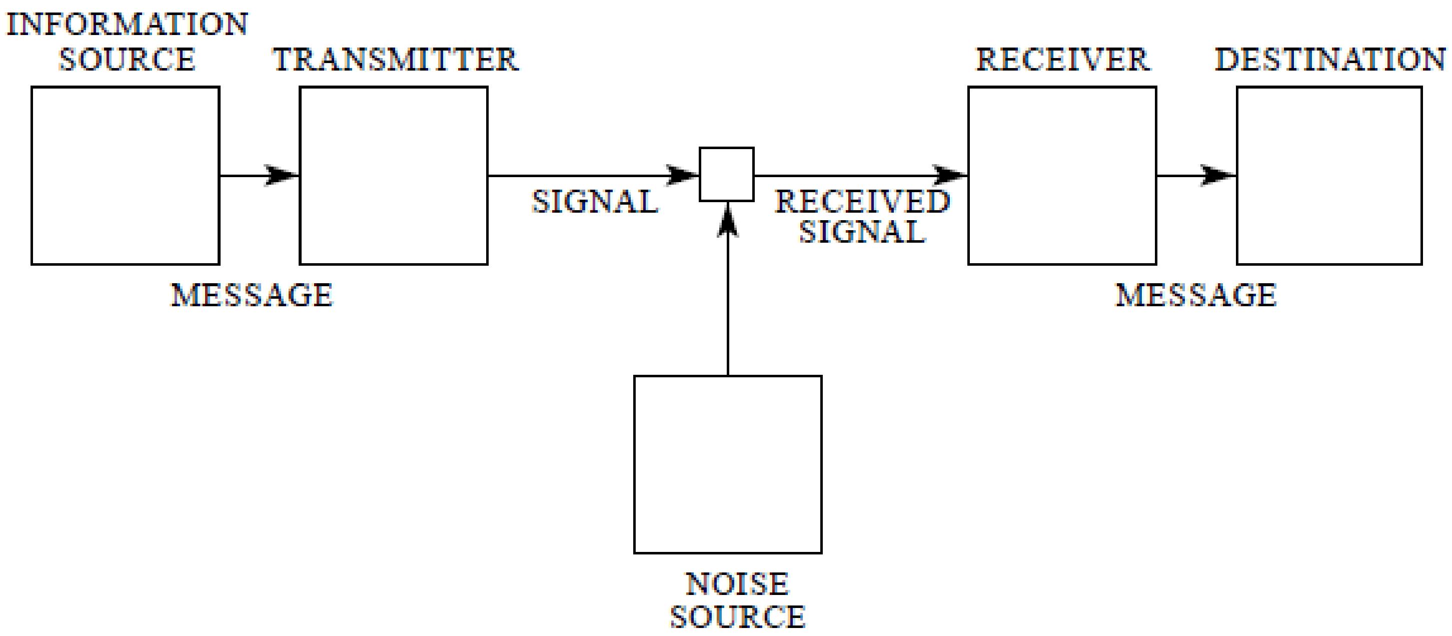
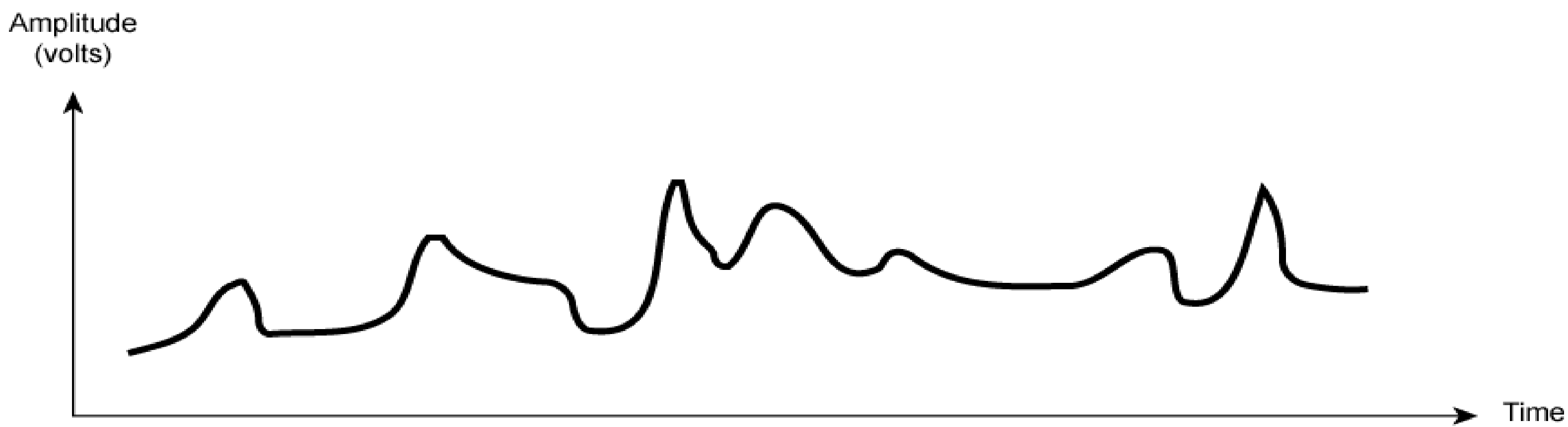


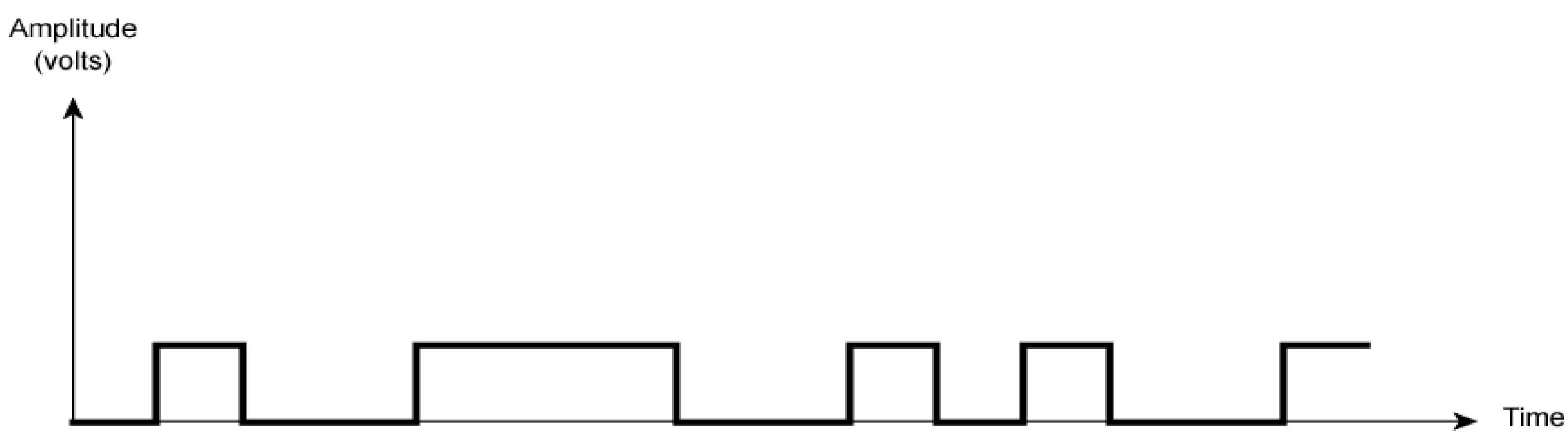
Fig. 1—Schematic diagram of a general communication system.

Figura tomada del articulo reeditado de Shannon

Señales : Analógicas y Digitales



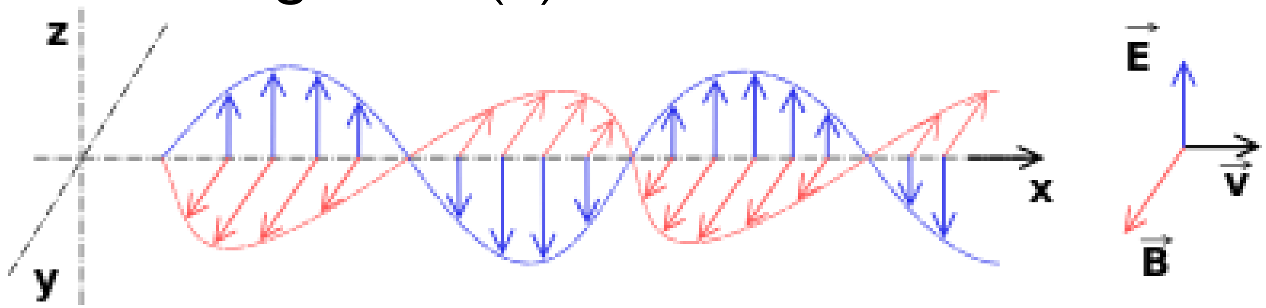
(a) Analog



(b) Digital

Fundamentos de las Señales

- Ondas electromagnéticas: dos campos ortogonales uno eléctrico (E) y el otro magnético (B).



- En el vacío se propagan a la velocidad de la luz (c)
  - Michelson-Morley demostraron que no existía el "éter"
- En otros medios se propagan a una velocidad menor, usualmente tomada como un factor de c.
  - Ejemplo: En un típico cable de red (UTP Cat. 5) el medio es el cobre, con $v \approx 0.69 * c$
- La luz puede considerarse una onda electromagnética.

Conceptos básicos: Ondas

- **Onda electromagnética:** es un campo eléctrico y uno magnético que se propagan juntos por un medio físico a una velocidad propia del medio.
  - En el caso del aire, la velocidad de propagación (casi) es la misma que la velocidad de la luz $c = 3*10^8$ m/s.
  - Vibra (oscila) a una frecuencia determinada (como un plano desplazándose longitudinalmente), con un comportamiento periódico en el eje de su propagación
  - Tienen un período (o repetición a longitudes constantes) que se denomina **Longitud de Onda** (λ) y se define $\boldsymbol{\lambda = c/f}$
    - Con **c** la velocidad de la luz y **f** la frecuencia de oscilación.
- **Problemas**: La onda, en el caso de chocar con imperfecciones del material, produce reflexiones, y además, si el medio tiene muchas pérdidas, se puede atenuar considerablemente.

Conceptos básicos: funciones periódicas

- Una ***función periódica*** $f(t)$ cumple que para todo valor de t:

$$f(t) = f(t + T).$$

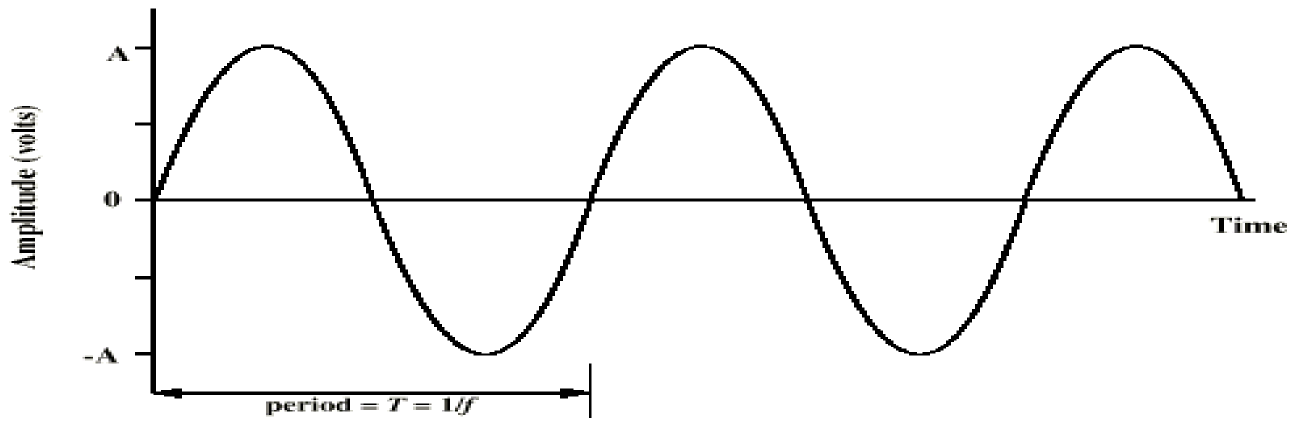
Al valor mínimo, mayor que cero, de la constante T que cumple lo anterior se le llama el ***período fundamental*** (o simplemente ***período***) de la función.

Se cumple:

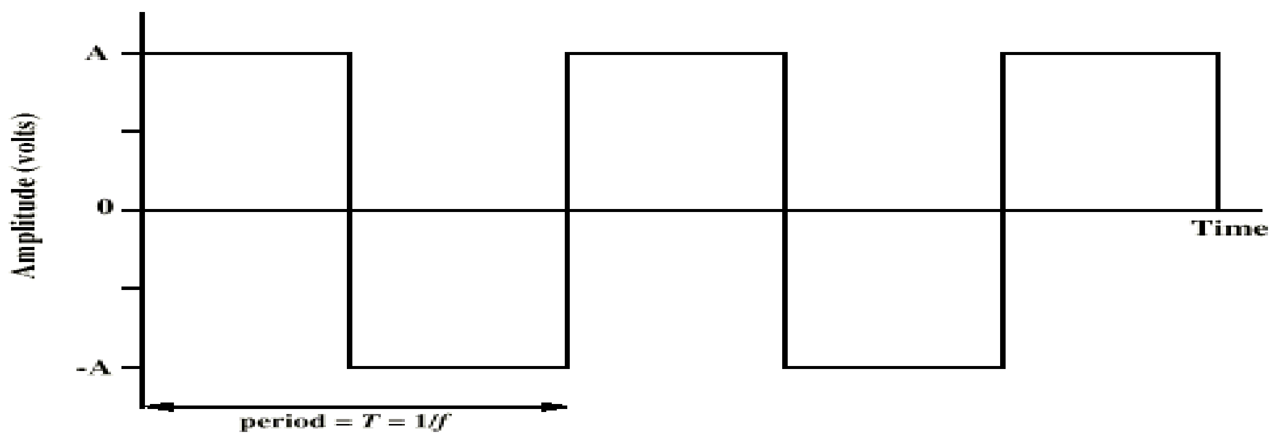
$$f(t) = f(t + \mathbf{n} * T), \text{ donde } n = 0, \pm 1, \pm 2, \pm 3, \ldots$$

- *Es $f(t)$ = cte. una función periódica?*

Señales Periódicas



(a) Sine wave

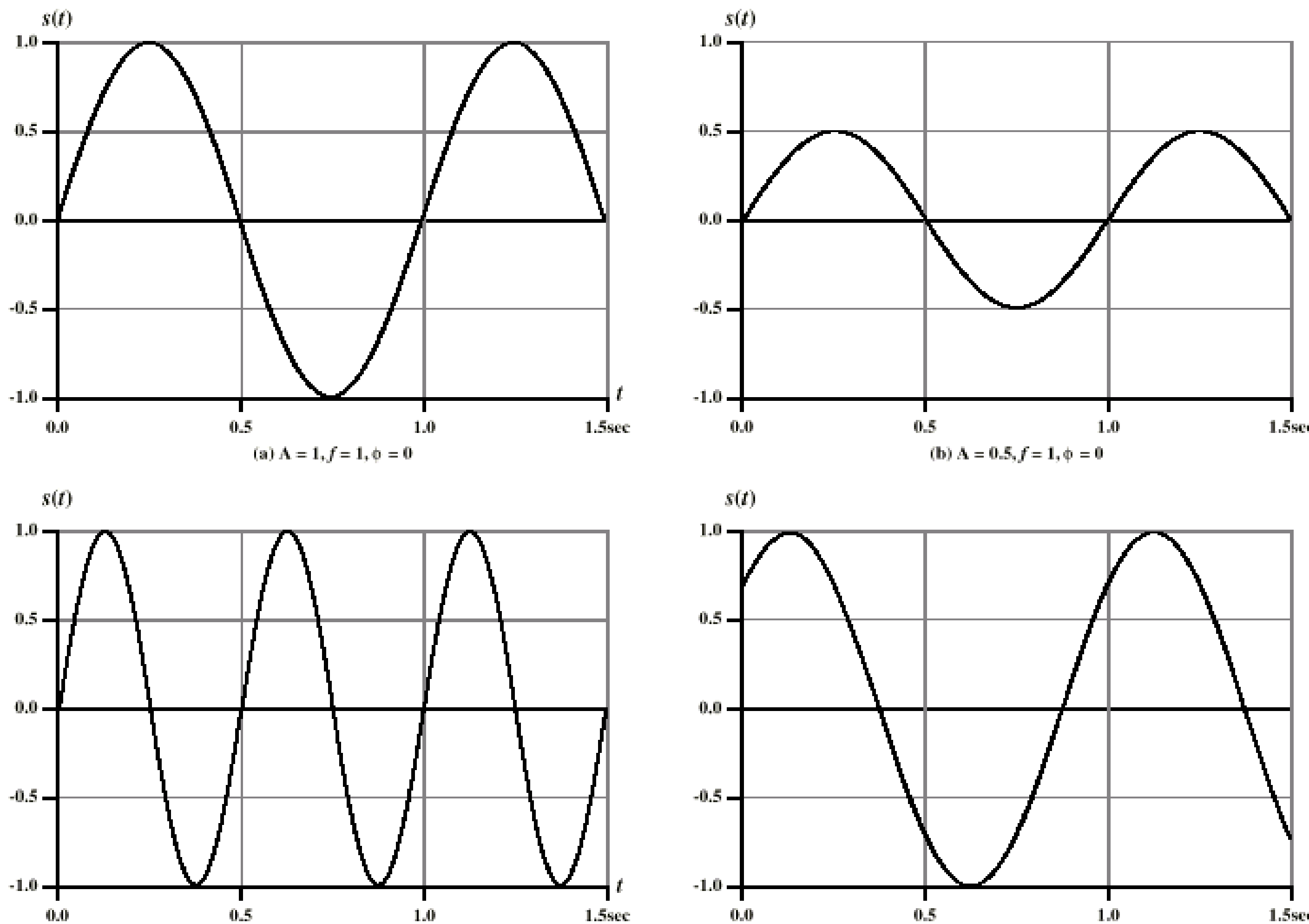


(b) Square wave

$s(t) = A * \mathrm{sen}(2\pi * f * t + \Phi)$

s(t)

s(t)



(a) A = 1, f = 1, ϕ = 0

(b) A = 0.5, f = 1, ϕ = 0

s(t)

s(t)

(c) A = 1, f = 2, ϕ = 0

(d) A = 1, f = 1, ϕ = π/4

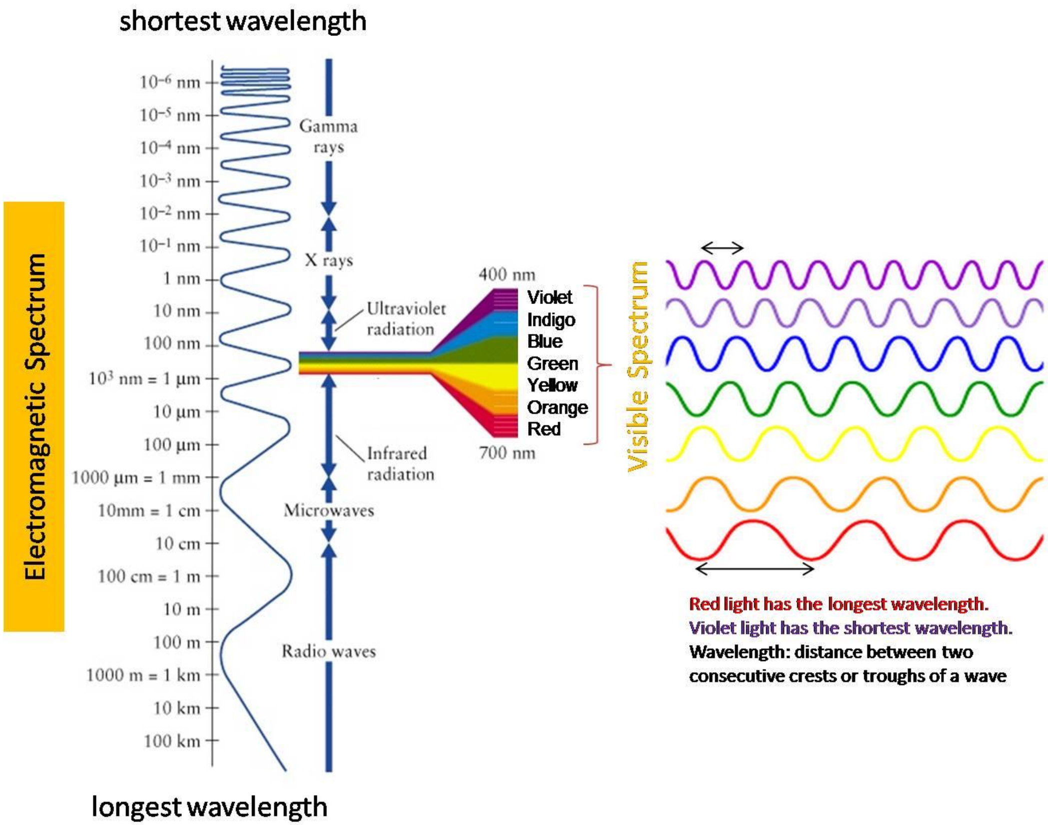
Onda Senoidal

- A = Amplitud
  - Amplitud (Magnitud física, ej.: Volts)
    - (ej: CA, A=310 Volt, Valor Eficaz = 220 Volt)
- w = Frecuencia Angular. $w = 2*\pi*f$
  - Radianes/segundo
- f = Frecuencia Temporal
  - Hertz (Hz) o ciclos/segundo
- T = Período
  - Tiempo en que se completa un ciclo de valores (T)
  - $T = 1/f$
- ϕ = Fase
  - Posición relativa (o desfasaje) en el tiempo

Longitud de Onda (λ)

- "Distancia ocupada" por un ciclo
- Distancia espacial entre dos puntos correspondientes a la misma fase,
  en dos ciclos consecutivos.
- En una onda *electromagnética*
  - Asumimos una velocidad lineal de propagación ***v***
  - $\lambda = \mathbf{v}.T = v / f$
  - $\lambda.f = \mathbf{v}$
- *Velocidad de la luz en el vacío*
  - v (luz en el vacío) = **c** = 3.10^8 m/s
  - *Longitud una onda de la luz en el vacío:* $\lambda = c / f$

El caso de las ondas de luz



Longitud una onda de la luz en el vacío: $\lambda = c / f$

Color	Wavelength	Frequency
violet	380–450 nm	668–789 THz
blue	450–495 nm	606–668 THz
green	495–570 nm	526–606 THz
yellow	570–590 nm	508–526 THz
orange	590–620 nm	484–508 THz
red	620–750 nm	400–484 THz

El dominio transformado

- Hasta ahora hemos representado las señales en el dominio del tiempo
- Sin embargo para comprender y/o simplificar la resolución del fenómeno de filtrado es conveniente pasar del dominio temporal al de la frecuencia.

Veremos dos herramientas :

1. Serie de Fourier
2. Transformada de Fourier

Serie trigonométrica de Fourier

- Funciones periódicas *f(t)* de periodo *T* pueden expresarse por la siguiente serie, llamada *serie trigonométrica de Fourier*

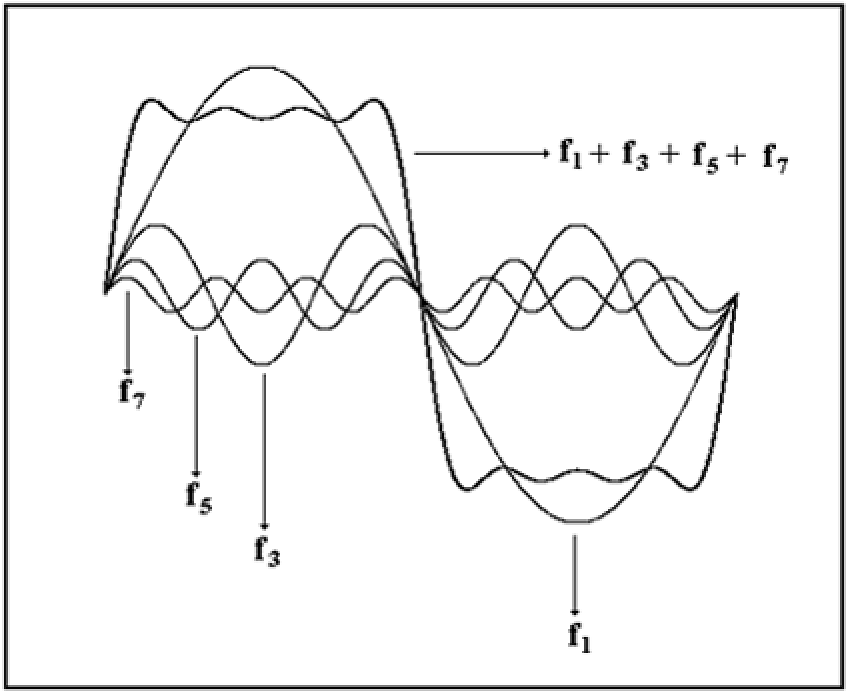
$$f(t) = \tfrac{1}{2}a_0 + a_1\cos(\omega_0 t) + a_2\cos(2\omega_0 t) + a_3\cos(3\omega_0 t) + \ldots$$
$$\ldots + b_1 sen(\omega_0 t) + b_2 sen(2\omega_0 t) + b_3 sen(3\omega_0 t) + \ldots$$

  - Donde $w_0 = 2\pi/T = 2\pi f_0$ se denomina frecuencia fundamental.

$$f(t) = \tfrac{1}{2}a_0 + \sum_{n=1}^{\infty}[a_n\cos(n\omega_0 t) + b_n sen(n\omega_0 t)]$$

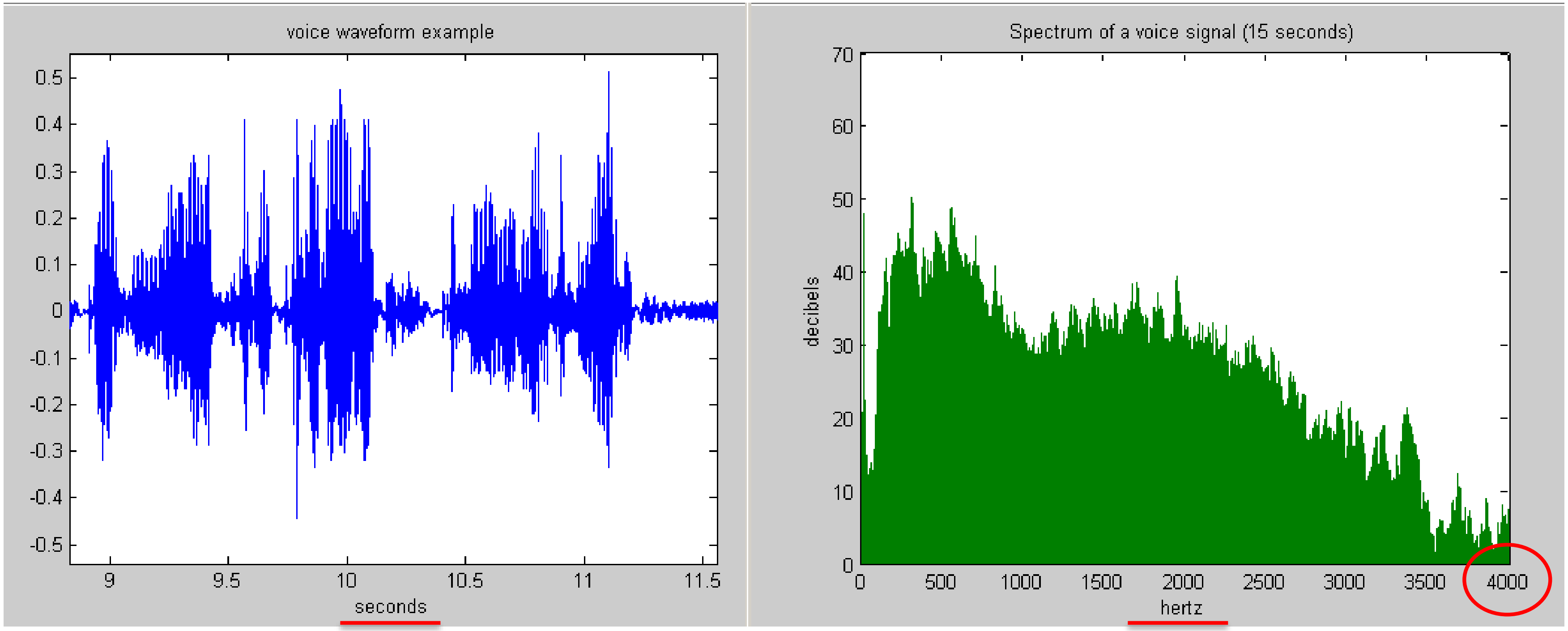
La onda Cuadrada

- Se puede representar como una serie infinita de senoides armónicamente relacionadas
  - fundamental
  - 1/3 tercera armónica
  - 1/5 quinta armónica
  - 1/7 séptima armónica
  - 1/9 novena armónica
  - etc….



Experimentos web interactivos:
http://www.intmath.com/fourier-series/fourier-graph-applet.php
http://betterexplained.com/articles/an-interactive-guide-to-the-fourier-transform/

Una señal vocal

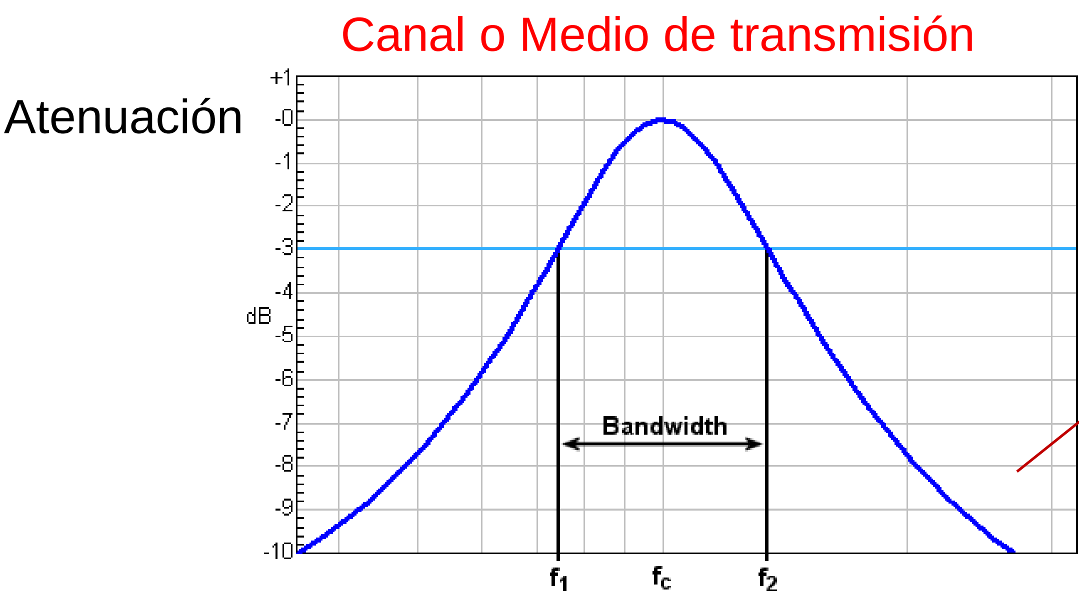


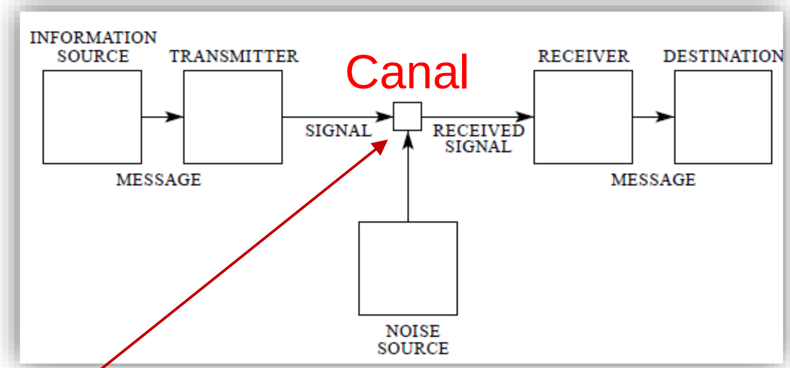
En el dominio del tiempo y de la frecuencia

http://commons.wikimedia.org/wiki/File:Voice_waveform_and_spectrum.png

Ancho de Banda

- “Experimento” en el pizarrón con una señal senoidal.





Formalmente la frecuencia de corte es donde se produce una **atenuación de 3 dB** (la próxima clase veremos atenuación)

Figura: http://es.wikipedia.org/wiki/Ancho_de_banda

"Mi mente divaga y concibo diferentes cosas día y noche. Como un escritor de ciencia ficción, estoy pensando, ¿y si fuera así?”

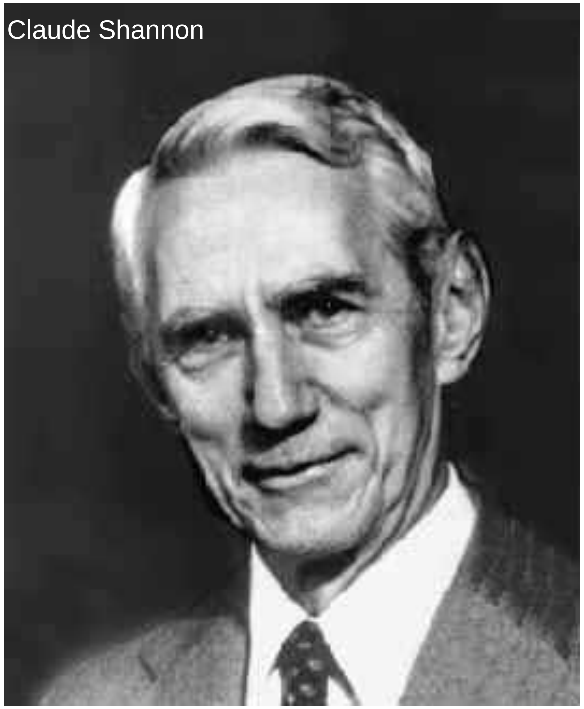
Claude Shannon

A MATHEMATICAL THEORY OF CRYPTOGRAPHY

- Proporcionó un análisis de los posibles "métodos criptográficos inquebrantables".
- Determinó qué "métodos secretos" serían ideales o más prácticos si no se pudiera implementar un "sistema inquebrantable".
- Proporcionó una prueba de que todos los " unbreakable ciphers" teóricamente "irrompibles" deben tener los mismos requisitos que el "one-time-pad" - un tratamiento fundamental de la criptografía moderna.
- Hizo una astuta observación de que el lenguaje, particularmente el inglés, era redundante y predecible.
- Se demostró que en un enlace punto a punto libre de errores donde un intruso "escucha" el mensaje transmitido sin error, con suficiente aleatoriedad común entre el transmisor y el receptor, se puede lograr un enlace de comunicación "perfectamente seguro".

A MATHEMATICAL THEORY OF COMMUNICATION

- Desarrollado a lo largo de los años de guerra, pero publicado en 1948, el documento de Shannon establece las bases para las comunicaciones digitales.
- Shannon argumentaba que todas las comunicaciones podían ser pensadas de la misma manera, ya fueran la radio, la televisión o el teléfono. Todos los mensajes, independientemente del canal, estaban potencialmente en riesgo de una entrega incorrecta debido al ruido. Para Shannon, la clave para superar el ruido y, por lo tanto, asegurar la entrega confiable de mensajes era la información contenida en el mensaje.
- Shannon escribió que el significado semántico de un mensaje era irrelevante para su transmisión. Un mensaje debe ser concebido como una secuencia con propiedades estadísticas. Son las estadísticas del mensaje las que podrían ser capturadas y su codificación minimizada para permitir una transmisión efectiva. Cuanto mayor es la entropía del mensaje, más esfuerzo se necesita para transmitirlo.



Teoría de la Información y Codificación

Introducción

Libro cabecera:
Norman Abramson. Teoría de la Información y la Codificación, 5ta. Ed., 1981

Teoría de la Información

- Claude Shannon estableció la Teoría Clásica de la Información
- También llamada teoría estadística de la información
  - Otra sería la teoría algorítmica de la información

Dos Teoremas Fundacionales:

1. Codificación para una fuente sin ruido
2. Codificación para un canal ruidoso

Teoría de Shannon

- Uno de ellos describe la máxima eficiencia posible de un método de corrección de errores (codificación) frente a los niveles de ruido y de corrupción de los datos.
  - No dice nada sobre como implementar dicha codificación.
- En definitiva brinda un límite teórico para la transmisión de bits (basándose en la Ley de los Grandes Números)

Shannon, paper de Bell Labs (1948)

A Mathematical Theory of Communication

By C. E. SHANNON

INTRODUCTION

THE recent development of various methods of modulation such as PCM and PPM which exchange bandwidth for signal-to-noise ratio has intensified the interest in a general theory of communication. A basis for such a theory is contained in the important papers of Nyquist[1] and Hartley[2] on this subject. In the present paper we will extend the theory to include a number of new factors, in particular the effect of noise in the channel, and the savings possible due to the statistical structure of the original message and due to the nature of the final destination of the information.

The fundamental problem of communication is that of reproducing at one point either exactly or approximately a message selected at another point. Frequently the messages have *meaning*; that is they refer to or are correlated according to some system with certain physical or conceptual entities. These semantic aspects of communication are irrelevant to the engineering problem. The significant aspect is that the actual message is one *selected from a set* of possible messages. The system must be designed to operate for each possible selection, not just the one which will actually be chosen since this is unknown at the time of design.

If the number of messages in the set is finite then this number or any monotonic function of this number can be regarded as a measure of the information produced when one message is chosen from the set, all choices being equally likely. As was pointed out by Hartley the most natural choice is the logarithmic function. Although this definition must be generalized considerably when we consider the influence of the statistics of the message and when we have a continuous range of messages, we will in all cases use an essentially logarithmic measure.

49

Información

Definición. Sea E un suceso que puede presentarse con probabilidad $P(E)$. Cuando E tiene lugar, decimos que hemos recibido

$$I(E) = \log \frac{1}{P(E)} \qquad (2\text{-}1)$$

unidades de información.

Información: unidades

Si introducimos el logaritmo de base 2, la unidad correspondiente se denomina *bit* *

$$I(E) = \log_2 \frac{1}{P(E)} \quad \text{bits} \tag{2-3a}$$

Empleando logaritmos naturales, la unidad de información recibe el nombre de *nat* **.

$$I(E) = \ln \frac{1}{P(E)} \quad \text{nats} \tag{2-3b}$$

En el caso de logaritmos de base 10, la unidad de información es el Hartley. R. V. Hartley fue quien primero sugirió la medida logarítmica de la información (Hartley, 1928).

$$I(E) = \log_{10} \frac{1}{P(E)} \quad \text{Hartleys} \tag{2-3c}$$

1 Bit

Notemos, también, que si $P(E) = 1/2$, será $I(E) = 1$ bit. Es decir, *un bit es la cantidad de información obtenida al especificar una de dos posibles alternativas igualmente probables*. Esta situación se presenta al lanzar una moneda al aire o al examinar la salida de un sistema de comunicación binario.

Fuente de memoria nula

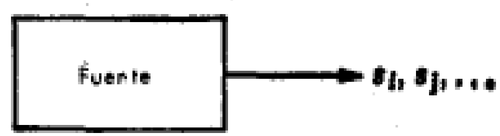


FIG. 2-1. Fuente de información.

Imaginemos la fuente emitiendo una secuencia de símbolos pertenecientes a un alfabeto finito y fijo, $S = \{s_1, s_2, \ldots, s_q\}$. Los símbolos emitidos sucesivamente se eligen de acuerdo con una ley fija de probabilidad. Ocasionalmente nos referimos a la fuente misma como S; sin que esto deba dar lugar a confusión. En la fuente más sencilla admitiremos que los símbolos emitidos son estadísticamente independientes. Tal fuente de información se conoce como *fuente de memoria nula* y puede describirse completamente mediante el alfabeto fuente S y las probabilidades con que los símbolos se presentan:

$$P(s_1),\ P(s_2),\ \ldots,\ P(s_q)$$

Memoria nula (cont)

Puede calcularse la información media suministrada por una fuente de información de memoria nula en la forma siguiente: La presencia de un símbolo s_i corresponde a una cantidad de información igual a

$$I(s_i) = \log \frac{1}{P(s_i)} \quad \text{bits}$$

Entropía

Para un símbolo s_i :

La probabilidad de que aparezca es precisamente $P(s_i)$, de modo que la cantidad *media* de informació– por símbolo de. la fuente es

$$\sum_S P(s_i)\, I(s_i) \quad \text{bits}$$

donde $\sum_S$ indica la suma extendida a q símbolos de la fuente S. Esta magnitud, cantidad media de información por símbolo de la fuente, recibe el nombre de *entropía* $H(S)$ de la fuente de memoria nula *.

$$H(S) \triangleq \sum_S P(s_i) \log \frac{1}{P(s_i)} \quad \text{bits} \qquad \text{(2-5a)}$$

Entropía (cont)

- Entropía de una fuente S de n mensajes s_i :

$$H(S) = \sum_{i=1}^{n} p(s_i).\log\frac{1}{p(s_i)} = -\sum_{i=1}^{n} p(s_i).\log p(s_i)$$

- Interpretaciones de H(S)
  - el *valor medio ponderado* de la cantidad de información del conjunto de mensajes posibles.
  - una medida de la incertidumbre promedio (grado de incerteza) acerca de una variable aleatoria
  - la cantidad de información obtenida al observar la aparición de cada nuevo símbolo

Entropía: Fuente Binaria

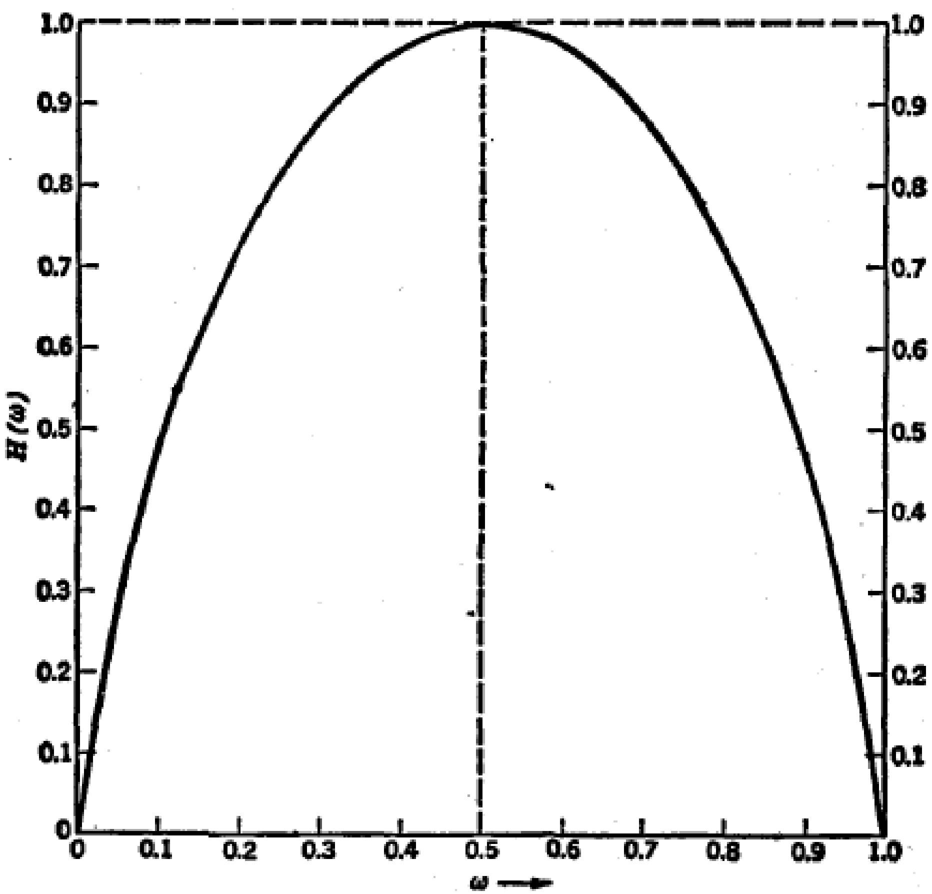


FIG. 2-3. $H(\omega)$, función entropía.

Propiedades de la entropía

a) La entropía es no negativa y se anula si y solo si un estado de la variable es igual a 1 y el resto 0.

b) La entropía es máxima (mayor incertidumbre del mensaje) cuando todos los valores posibles de la variable **s** son equiprobables.

Si hay n estados equiprobables, entonces $p_i = 1/n$

Luego:

$$\mathbf{H(S)} = - \Sigma\, p_i \log_2 p_i = - n(1/n) \log_2 (1/n) =$$

$$= - (\log_2 1 - \log_2 n)$$

$$= \log_2 n = \mathbf{H(S)}_{\text{máx}}$$

Extensión a una Fuente de Memoria Nula

$$H(S^n) = n\,H(S) \qquad (2\text{-}18)$$

Ejemplo 2-2. Consideremos la extensión de segundo orden de la fuente del ejemplo 2-1. Recordemos que la fuente tenía un alfabeto $S = \{s_1, s_2, s_3\}$, con $P(s_1) = 1/2$ y $P(s_2) = P(s_3) = 1/4$. Así la fuente S^2 tendrá los nueve símbolos siguientes:

Símbolos de S^2	σ_1	σ_2	σ_3	σ_4	σ_5	σ_6	σ_7	σ_8	σ_9
Secuencia correspondiente a los símbolos de S	s_1s_1	s_1s_2	s_1s_3	s_2s_1	s_2s_2	s_2s_3	s_3s_1	s_3s_2	s_3s_3
Probabilidad $P(\sigma_i)$	1/4	1/8	1/8	1/8	1/16	1/16	1/8	1/16	1/16

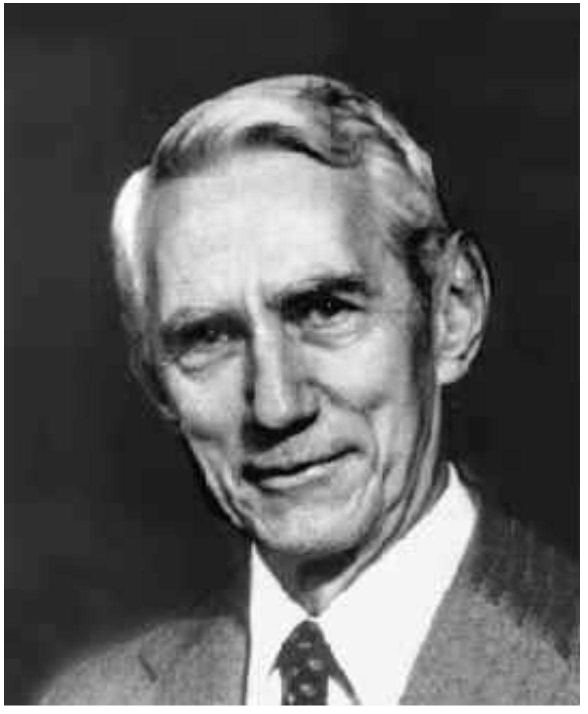
$$H(S^2) = \sum_{S^2} P(\sigma_i) \log \frac{1}{P(\sigma_i)}$$

$$= 1/4 \log 4 + 4 \times 1/8 \log 8 + 4 \times 1/16 \log 16$$

$$= 3 \text{ bits/símbolo}$$

Agenda (Parte 3)

- Introducción a la Teoría de la Información
  - Codificación
  - Códigos óptimos
  - Huffman



Teoría de la Información y Codificación

Codificación

Claude Shannon

Consideremos un código instantáneo con un alfabeto fuente

$$S = \{s_1, s_2, \ldots, s_q\}$$

y un alfabeto código $X = \{x_1, x_2, \ldots, x_r\}$. Sean $X_1, X_2, \ldots, X_q$ las palabras del código y, por definición, l_i la longitud (es decir, el número de símbolos del código) de la palabra X_i. Normalmente es interesante que las longitudes de las palabras del código sean lo más cortas posible. La condición necesaria y suficiente para que exista un código instantáneo con palabras de longitud $l_1, l_2, \ldots, l_q$, viene definida por la *inecuación de Kraft* (Kraft, 1949).

> La condición necesaria y suficiente para la existencia de un código instantáneo de longitudes $l_1, l_2, \ldots, l_q$ es que
>
> $$\sum_{i=1}^{q} r^{-l_i} \leq 1$$
>
> donde r es el número de símbolos diferentes que constituyen el alfabeto código.

En el caso de alfabeto binario, la inecuación de Kraft se transforma en

$$\sum_{i=1}^{q} 2^{-l_i} \leq 1 \qquad (3\text{-}3)$$

donde la suma se extiende a todas las palabras del código bloque. Antes de probar esta inecuación, es interesante ver en qué forma puede

Codificación

- Establecer una correspondencia entre los símbolos de una fuente y los símbolos del alfabeto de un código.

- Proceso mediante el cual también podemos lograr una representación eficiente de la información (eliminar redundancia).

Codificación: condiciones

- Bloque
- Singular
- Separable (unívocamente decodificable)

Condición de los prefijos

- La condición *necesaria y suficiente* para que un código sea *instantáneo* es que sus palabras cumplan la condición de los prefijos:
- No exista palabra que sea prefijo de otra palabra de longitud mayor.

Códigos eficientes

- Asignar palabras más cortas a símbolos más probables
  - **l_i :** longitud de la palabra codificada del mensaje m_i
  - **r :** # de símbolos del alfabeto del código
- **$L = \sum p_i l_i$** : Longitud media de un código
- $L \log r \geq H(s)$

- log r : Cantidad promedio máxima de información de un símbolo del código
- **$h = H(S) / (L \log r)$** Eficiencia del código

Si exigimos que el código sea instantáneo, la inecuación de Kraft impone que el argumento del segundo logaritmo del segundo miembro de (4-6) sea igual o menor que la unidad. Por lo tanto, su logaritmo deberá ser igual o menor que cero, y

$$H(S) \leq L \log r \tag{4-7a}$$

o bien

$$\frac{H(S)}{\log r} \leq L \tag{4-7b}$$

$H(S)$ viene medida en bits en la ecuación (4-7*b*). Recordemos que L es el número medio de símbolos utilizados para codificar S. Expresando la entropía asimismo en unidades r-arias, como en (2-5*c*), la relación (4-7*b*) podría escribirse en la forma

$$H_r(S) \leq L \tag{4-7c}$$

Ejemplo 2-1. Consideremos la fuente $S = \{s_1, s_2, s_3\}$ con $P(s_1) = 1/2$ y $P(s_2) = P(s_3) = 1/4$. Entonces

$$H(S) = 1/2 \log 2 + 1/4 \log 4 + 1/4 \log 4$$
$$= 3/2 \text{ bits}$$

Si medimos $I(s_i)$ en unidades de orden r, $H(S)$ vendrá dada en la misma unidad, y tendremos

$$H_r(S) = \sum_S P(s_i) \log_r \frac{1}{P(s_i)} \quad \text{unidades de orden } r \tag{2-5b}$$

De la ecuación (2-2) se deduce

$$H_r(S) = \frac{H(S)}{\log r} \tag{2-5c}$$

$$\log_a x = \frac{1}{\log_b a} \log_b x \tag{2-2}$$

Codificador óptimo

Nos falta encontrar el segundo término pendiente en la definición de cantidad de información: *codificador óptimo*.

Introduciendo el signo negativo dentro del logaritmo en la expresión de la entropía, ésta nos quedará como:

$$\boxed{H(X) = \Sigma \; p(x) \log_2 [1/p(x)]}$$

La expresión $\log_2 [1/p(x)]$ representa el número de bits necesario para codificar el mensaje X en un codificador óptimo.

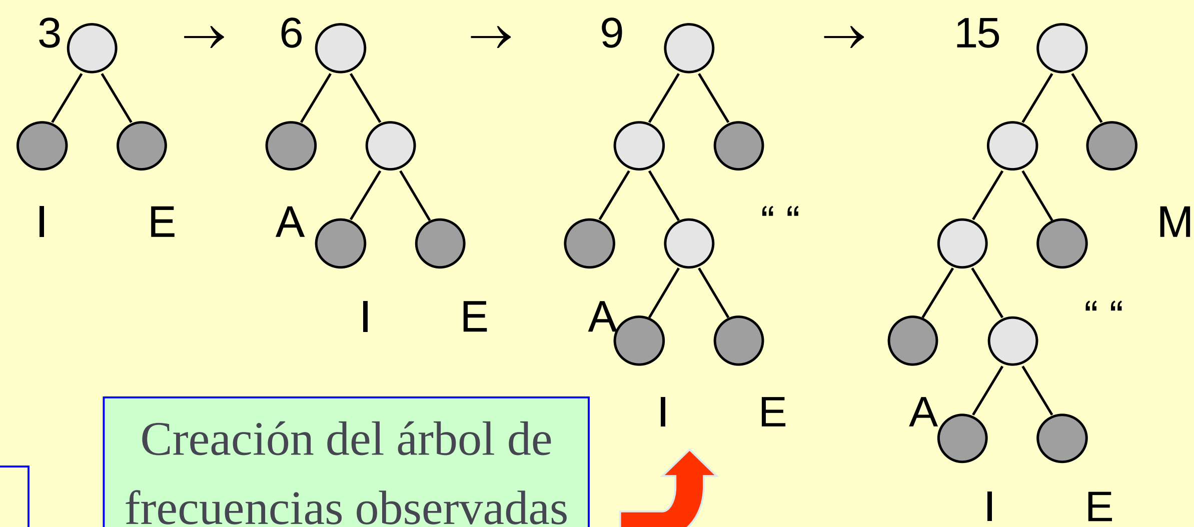
Codificador óptimo es aquel que para codificar un mensaje X usa el menor número posible de bits.

Codificación de Huffman

Mensaje: MI MAMA ME MIMA

Letra	Frecuencia
E	1 vez
I	2 veces
A	3 veces
“ “	3 veces
M	6 veces

Ocurrencias →



Creación del árbol de frecuencias observadas

Código óptimo:

M = 1 “ ” = 01 A = 000 I = 0010 E = 0011

Mensaje: 1 0010 01 1 000 1 000 01 1 0011 01 1 0010 1 000 (33 bits)

Pregunta: ¿Con cuántos bits se codificaría si se usara ASCII? Saque conclusiones.

Agenda (Parte 3)

- Introducción a la Teoría de la Información
  - Visión integradora de los teoremas fundamentales de Shannon

Los medios de transmisión

Sus perturbaciones y no idealidades

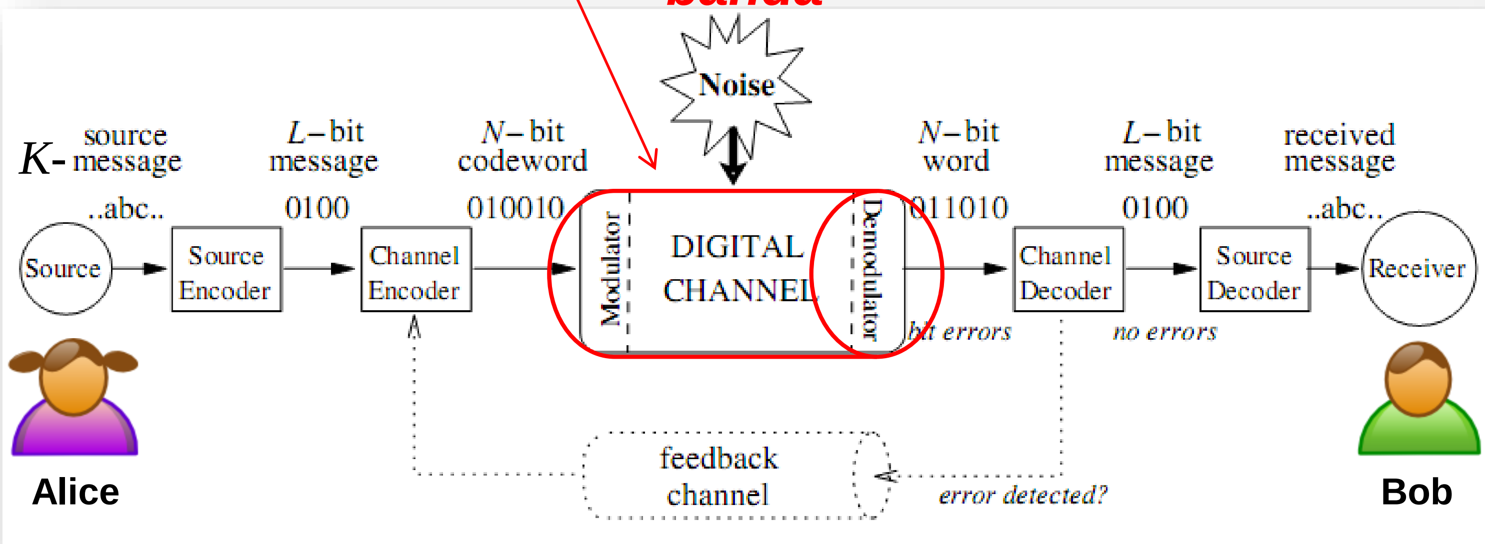
Modelo de un Sistema de Comunicaciones

Sistema de Comunicación ideal:

Modelo de un Sistema de Comunicaciones

Sistema de Comunicación <u>real</u>:

Canal sometido a ruido, limitado en potencia y en ancho de banda



Perturbaciones en la transmisión

- La señal recibida puede diferir de la señal transmitida
- Analógico - degradación de la calidad de la señal
- Digital - Errores de bits
- Causado por
  - Atenuación y distorsión de atenuación
  - Distorsión de retardo
  - Ruido

Atenuación

- La intensidad de la señal disminuye con la distancia
- Depende del medio
- La intensidad de la señal recibida:
  - Debe ser suficiente para que se detecte
  - Debe ser suficientemente mayor que el ruido para que se reciba sin error
  - Se ve más afectada a mayores frecuencias
- Ecualización: amplificar más las frecuencias más altas
- Problema "menos grave" para las señales digitales

Distorsión de retardo

- Solo en medios guiados
- La velocidad de propagación en el medio varía con la frecuencia
- Las componentes de frecuencia llegan al receptor en distintos instantes de tiempo, originando desplazamientos de fase entre las distintas frecuencias
- Para una señal limitada en frecuencia, la velocidad es mayor cerca de la frecuencia central

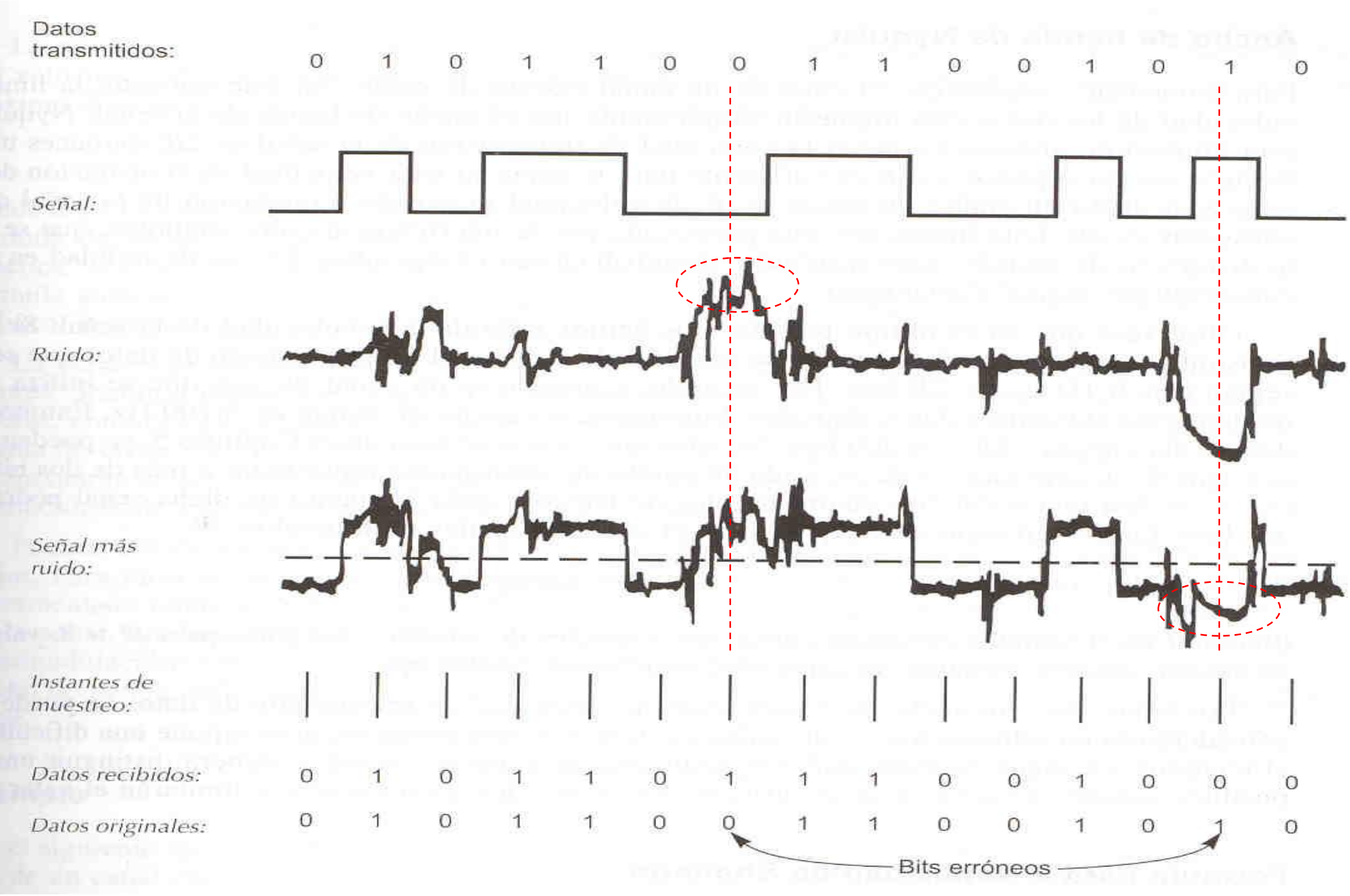
Ruido (1)

- Señales adicionales insertadas entre el transmisor y el receptor
- Térmico
  - Debido a la agitación térmica de los electrones
  - Aumenta linealmente con la temperatura absoluta (N_0=k.T)
  - Uniformemente distribuido en la frecuencia =>
    - Densidad de Potencia del Ruido Blanco (N_B= N_0.B= k.T.B)
- Intermodulación
  - Señales que son la suma y la diferencia de frecuencias originales y sus múltiplos ($mf_1 \pm nf_2$)
  - Se produce por falta de linealidad en el canal

Ruido (2)

- Diafonía
  - Una señal de una línea interfiere en otra
- Impulsivo
  - Impulsos irregulares o picos
  - Ej: Interferencia electromagnética externa (tormenta)
    - Corta duración
    - Gran amplitud
    - Disruptivo

Efecto del ruido en señal digital



Conceptos relacionados con la capacidad del canal

- Velocidad de transmisión de datos **C**
  - En bits por segundo
- Ancho de Banda **B**
  - En ciclos por segundo (Hertz)
  - Limitado por el transmisor y el medio
- Ruido **N**
  - Nivel medio a través del canal de transmisión
- Tasa de errores **BER**
  - Cambiar 0 por 1, o viceversa
  - Cantidad de veces que esto sucede por unidad de tiempo
  - BER: Bit Error Rate

Ancho de Banda de Nyquist (Capacidad teórica máxima sin ruido)

Para símbolos de 2 niveles SIN RUIDO

- Velocidad binaria

$$C(bps) = 2B(Hz)$$

Para símbolos de M niveles SIN RUIDO

- Velocidad binaria

$$C(bps) = 2B(Hz)\log_2 M$$

- *1 Baudio = 1 estado señalización/seg (también se expresa símbolos/seg)*
- *1 Baudio = 1 bps si M=2, 2 bps si M=4, etc.*
- *La relación entre la* ***velocidad de transmisión C*** *y la* ***velocidad de modulación V*** *es:*

$$C(bps) = V(baudios)\cdot\log_2 M$$

$$C(bps) = V\cdot\log_2 M = 2\cdot B\cdot\log_2 M = B\cdot\log_2 M^2$$

 Nyquist, H., "Certain Factors Affecting Telegraph Speed," *Bell System Technical Journal,* April 1924, p. 324; "Topics in Telegraph Transmission Theory," *A.I.E.E. Trans.*, v. 47, April 1928, p. 617.

Capacidad de Shannon (1)

- Para un cierto Nivel de Ruido, a mayor velocidad C:
  - menor período de un bit
  - mayor tasa de error (se pueden corromper 2 bits en el tiempo en que antes se corrompía 1 bit)
- Relación Señal a Ruido (Signal-Noise Ratio, SNR):

$$SNR_{dB} = 10\log_{10}(SNR) = 10\log_{10}\frac{Potencia\_Señal}{Potencia\_Ruido}$$

- Veamos:

Capacidad de Shannon (2)

- En principio, si se aumentan el ancho de banda ***B*** y la potencia de señal ***S***, aumenta la velocidad binaria ***C***
- Pero:
  - Un aumento del ancho de banda ***B*** aumenta el ruido
  - Un aumento de potencia de señal ***S*** aumenta las no linealidades y el ruido de intermodulación
- Según Shannon, la velocidad binaria teórica máxima para un canal será:

$$C_{máx}(bps) = B(Hz) \cdot \log_2(1 + SNR)$$

Capacidad de Shannon (3)

- Nyquist:

$$C(bps) = V \cdot \log_2 M = 2 \cdot B \cdot \log_2 M = B \cdot \log_2 M^2$$

- Shannon:

$$C_{máx}(bps) = B \cdot \log_2(1 + SNR)$$

- => Restricción: no se podrá aumentar *M* tanto como se quiera:

$$M \leq \sqrt{1 + SNR}$$

Ejemplo

- Canal entre 3 MHz y 4 MHz
- Relación señal ruido = 24 dB, $SNR=10^{(24/10)}=251$

Calcular ancho de banda

- Respuesta: ***B*** = 1 MHz

Calcular la velocidad binaria teórica máxima y el número de niveles

- Respuesta: ***C*** = 8 Mbps
- Respuesta: ***M*** = 16 niveles

Visión integradora de la Teoría de la Información

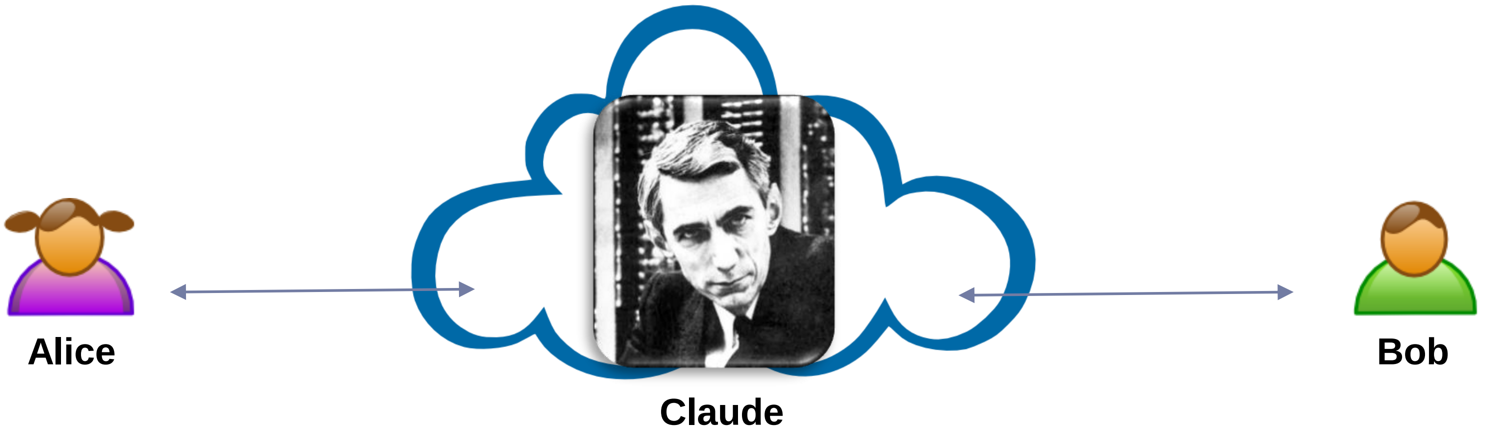
- "Límites fundamentales" y "Resultados no intuitivos"

  - ¿Cual es la complejidad irreducible por debajo de la cual una señal que debe ser transmitida no puede ser compactada sin pérdida de información? (límite de la **eficiencia**)

  - ¿Cual es el límite absoluto de la tasa de transmisión utilizada para transportar una señal de manera confiable a través de un canal ruidoso? (límite de la **confiabilidad**)

- Estos aspectos se reflejan en aplicaciones prácticas.

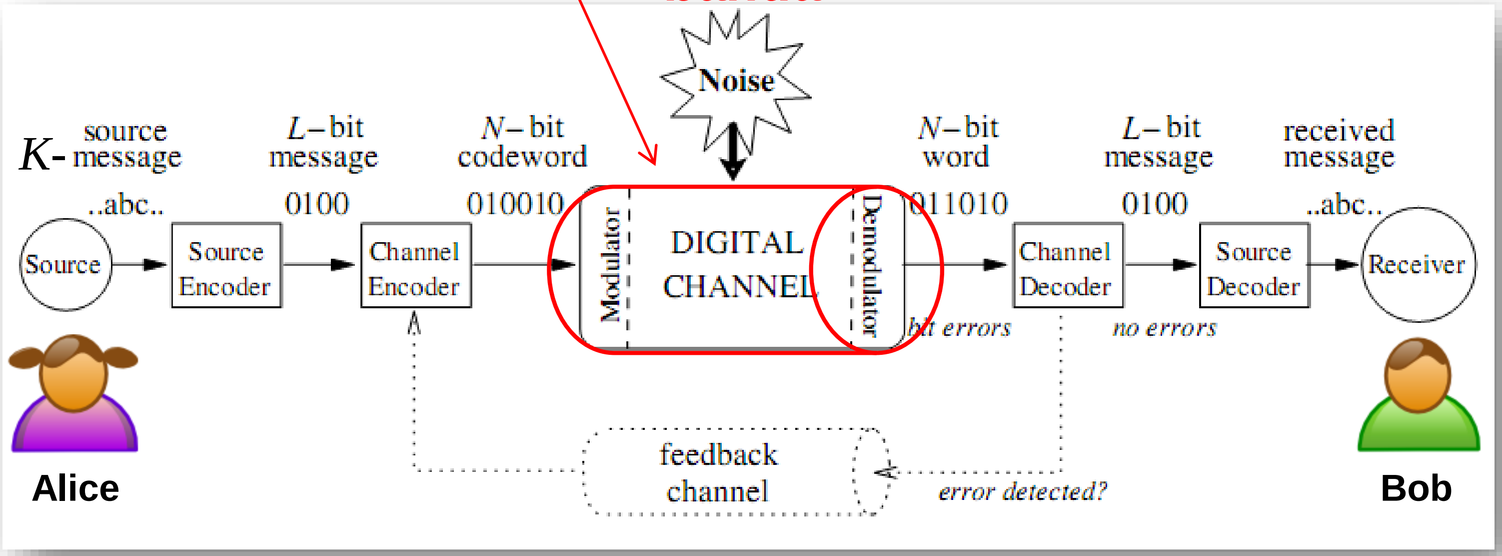
Marco de Referencia



Marco de Referencia

Sistema de Comunicación <u>real</u>:

Canal sometido a ruido, limitado en potencia y en ancho de banda



Bibliografía

- Principles of Digital Communication, Robert G. Gallager. Cambridge University Press, 2008.
- Communication Systems, Simon Haykin. Cuarta Edición, John Wiley & Sons, 2001.
- Information Theory and Coding, Norman Abramson. Primera Edición, McGraw Hill, 1963.
- How Claude Shannon and the Bell Labs Mathematics Department founded the digital age.

https://www.bell-labs.com/claude-shannon/

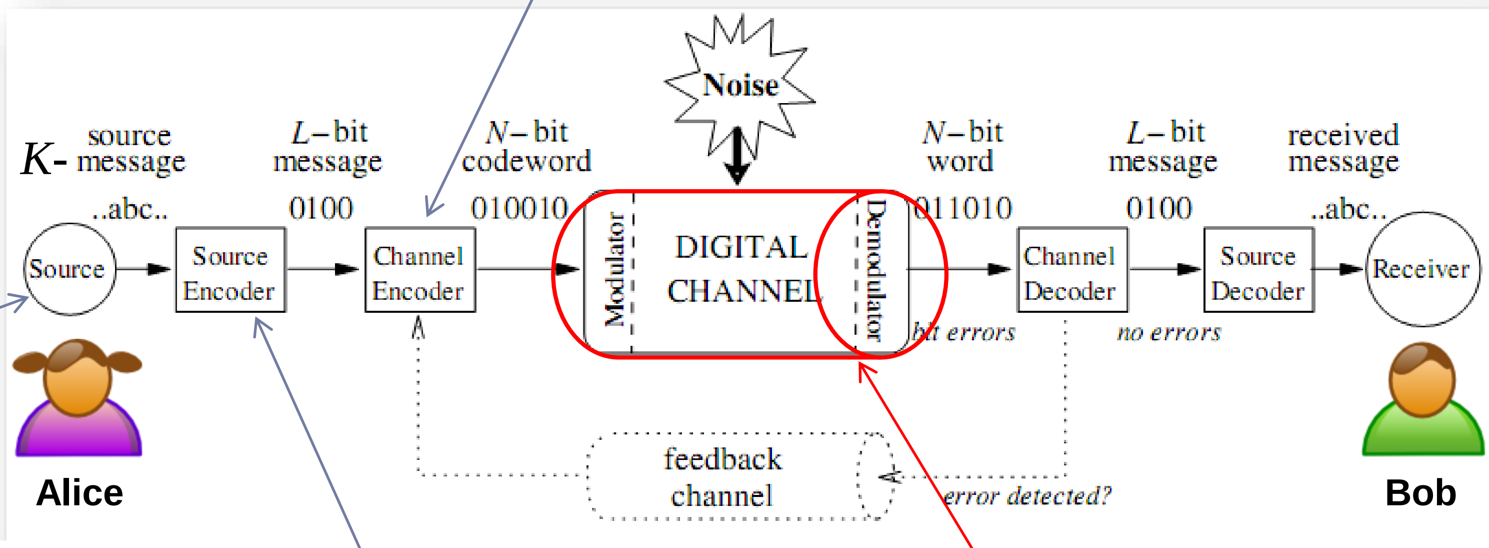
Extras

Marco de Referencia

3° Teorema de Codificación de Canal

Comunicación **Confiable** (error bajo control)

$$\frac{H(\mathcal{S})}{T_s} \leq \frac{C}{T_c}$$



1° Conceptos Básicos

$$I = log_2(\frac{1}{p_k})$$

$$H = \sum_{k=0}^{K-1} p_k . log_2(\frac{1}{p_k})$$

Información y Entropía

$0 \leq H(S) \leq \log_2 K$

$$\bar{L} \geq H(\mathcal{S})$$

2° Teorema de Codificación de Fuente

Comunicación **Eficiente**

$$C = B.log_2(1 + \frac{S}{N})$$

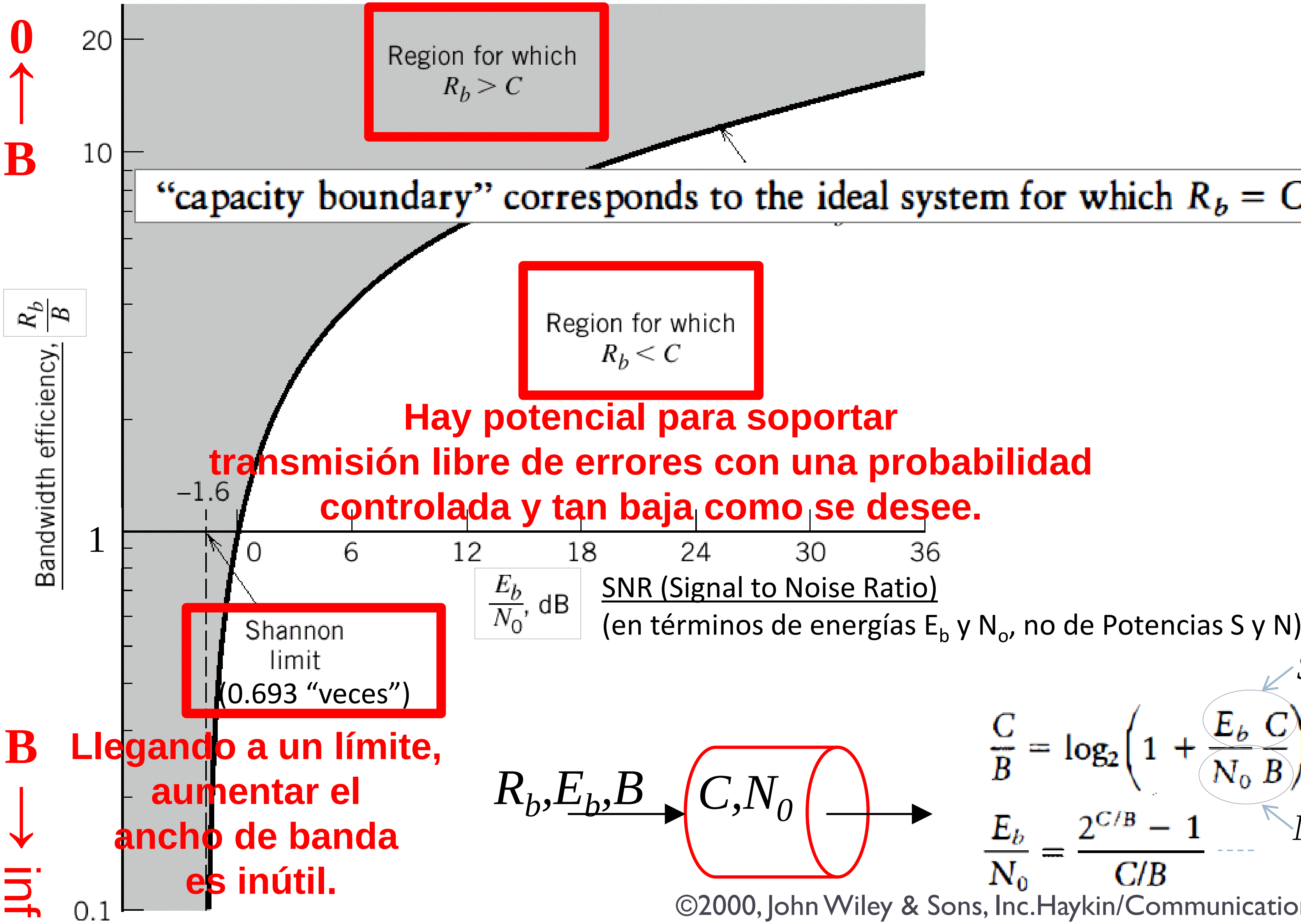
4° Teorema de Capacidad de Información

Compromiso Ancho de banda vs Relación Señal a Ruido

Diagrama de “Eficiencia del Ancho de Banda”

El sistema está condenado a tener una muy alta probabilidad de errores, sin posibilidad de control.

Válido para cualquier algoritmo que se use para la Codificación y Decodificación de canal.



$$\frac{C}{B} = \log_2\left(1 + \frac{E_b}{N_0}\frac{C}{B}\right)$$

S

N

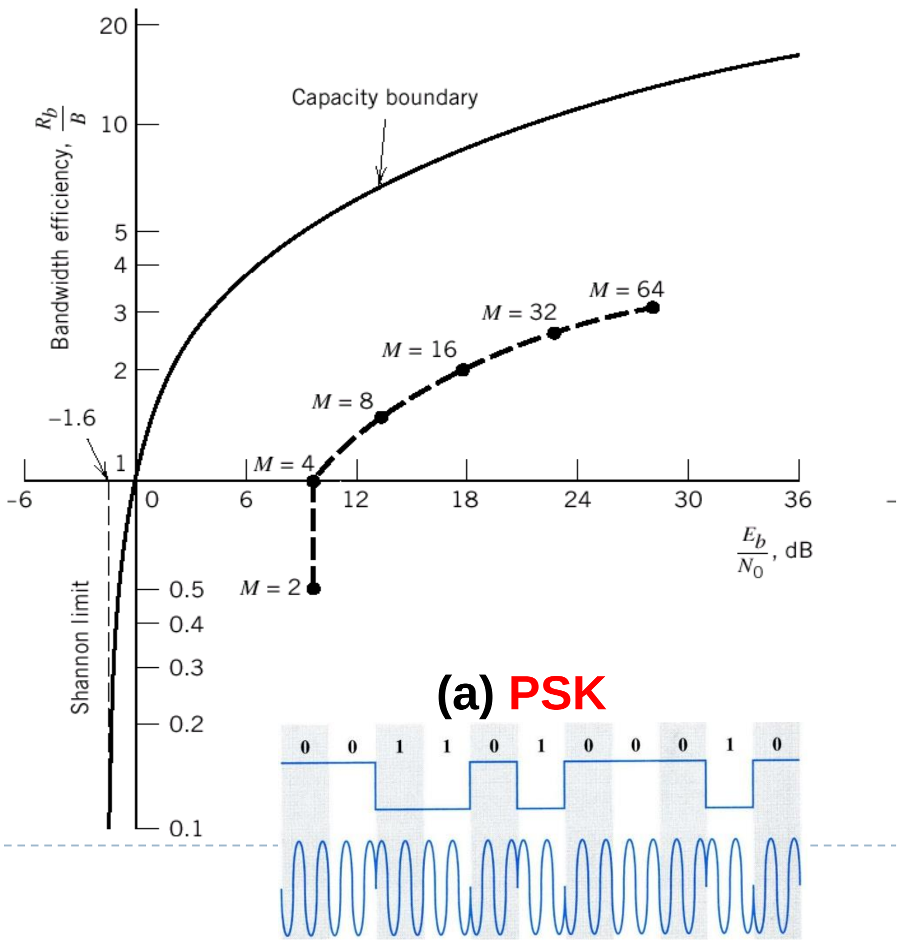
$$\frac{E_b}{N_0} = \frac{2^{C/B} - 1}{C/B}$$

Ejemplos del mundo real: Modulaciones.

Contra el **sistema ideal** para $P_e = 10^{-5}$ y M creciente.

(*a*) Comparison of *M*-ary **PSK (Phase Shift Keying)**

(*b*) Comparison of *M*-ary **FSK (Frequency Shift Keying)**



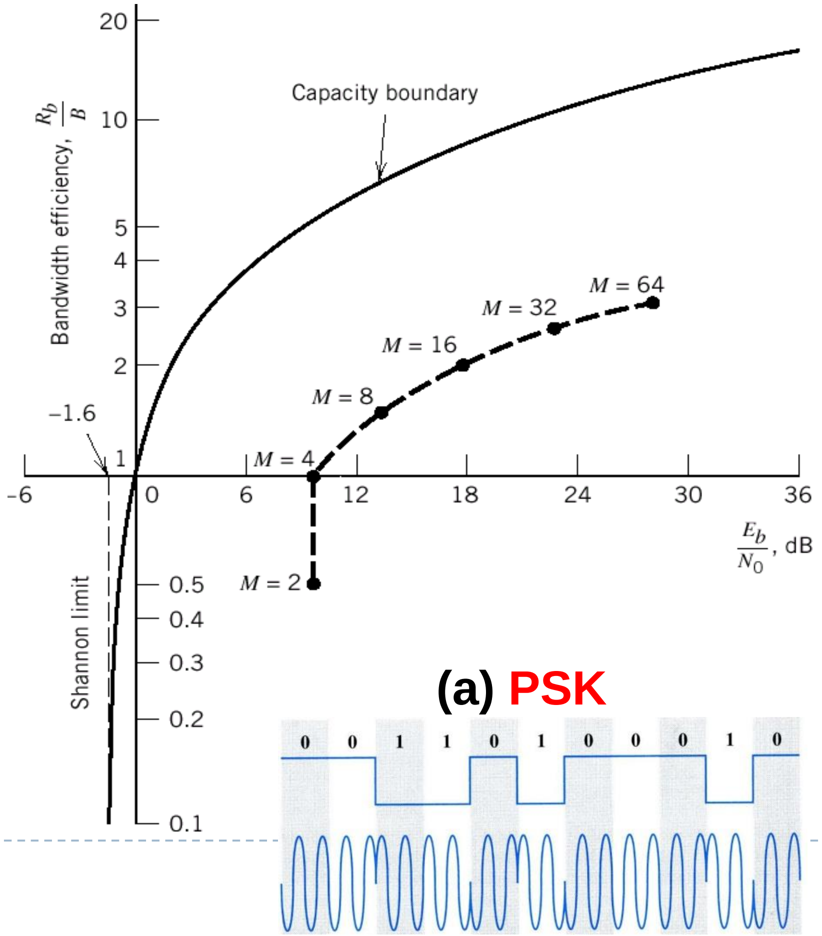
(a) PSK

Ejemplos del mundo real: Modulaciones.

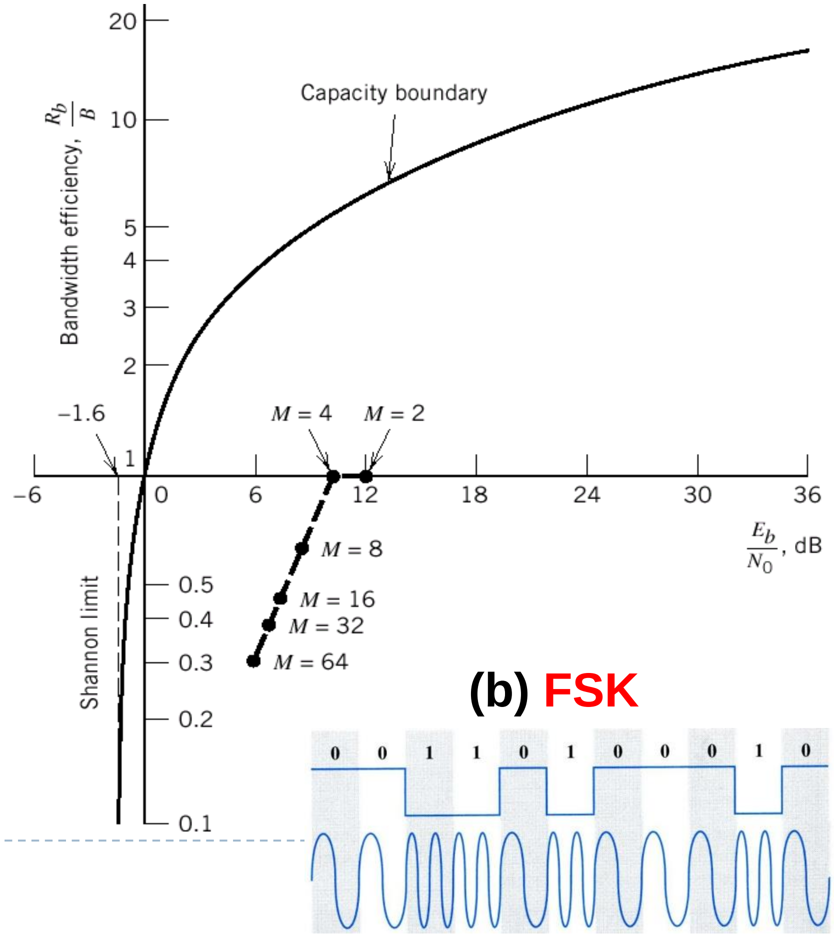
Contra el **sistema ideal** para $P_e = 10^{-5}$ y M creciente.

(*a*) Comparison of *M*-ary **PSK (Phase Shift Keying)**

(*b*) Comparison of *M*-ary **FSK (Frequency Shift Keying)**



(a) PSK



(b) FSK

C. E. Shannon, Bell System Technical Journal, vol. 27, pp. 379-423 and 623-656, July and October, 1948

“A method is developed for representing any communication system geometrically. Messages and the corresponding signals are points in two “function spaces,” and the modulation process is a mapping of one space into the other. Using this representation, a number of results in communication theory are deduced concerning expansion and compression of bandwidth and the threshold effect. Formulas are found for the maximum rate of transmission of binary digits over a system when the signal is perturbed by various types of noise. Some of the properties of “ideal” systems which transmit at this maximum rate are discussed. The equivalent number of binary digits per second for certain information sources is calculated. “

C. E. Shannon (January 1949). "Communication in the presence of noise" *Proc. Institute of Radio Engineers* **vol. 37** (1): 10–21.

The recent development of various methods of modulation such as PCM and PPM which exchange bandwidth for signal-to-noise ratio has intensified the interest in a general theory of communication. A basis for such a theory is contained in the important papers of Nyquist and Hartley on this subject. In the present paper we will extend the theory to include a number of new factors, in particular the effect of noise in the channel, and the savings possible due to the statistical structure of the original message and due to the nature of the final destination of the information.

The fundamental problem of communication is that of reproducing at one point either exactly or approximately a message selected at another point. Frequently the messages have meaning; that is they refer to or are correlated according to some system with certain physical or conceptual entities. These semantic aspects of communication are irrelevant to the engineering problem. The significant aspect is that the actual message is one selected from a set of possible messages. The system must be designed to operate for each possible selection, not just the one which will actually be chosen since this is unknown at the time of design. If the number of messages in the set is finite then this number or any monotonic function of this number can be regarded as a measure of the information produced when one message is chosen from the set, all choices being equally likely. As was pointed out by Hartley the most natural choice is the logarithmic function. Although this definition must be generalized considerably when we consider the influence of the statistics of the message and when we have a continuous range of messages, we will in all cases use an essentially logarithmic measure.

Fuente de Markov

$$P(s_i/s_{i_1}, s_{i_2}, \ldots, s_{i_m}) \quad \text{para} \quad i = 1, 2, \ldots, q; \; i_p = 1, 2, \ldots, \tag{2-19}$$

En una fuente de Markov de orden m, la probabilidad de un símbolo cualquiera viene determinada por los m símbolos que lo preceden. En cualquier momento, por lo tanto, definiremos el *estado* de la fuente de Markov de orden m por los m símbolos precedentes. Puesto que existen q símbolos distintos, una fuente de Markov de orden m admitirá q^m estados posibles. Al emitir la fuente nuevos símbolos, el estado cambia. Un procedimiento simple de estudiar el comportamiento de la fuente consiste en utilizar un *diagrama de estados*. En este diagrama cada uno de los q^m estados posibles de la fuente se representa por un punto, indicándose mediante flechas las transiciones entre estados.

Fuente de Markov (cont)

Ejemplo 2-3. Consideremos una fuente de Markov de segundo orden con un alfabeto binario $S = \{0,1\}$. Supongamos que las probabilidades condicionales son

$$P(0/00) = P(1/11) = 0.8$$

$$P(1/00) = P(0/11) = 0.2$$

$$P(0/01) = P(0/10) = P(1/01) = P(1/10) = 0.5$$

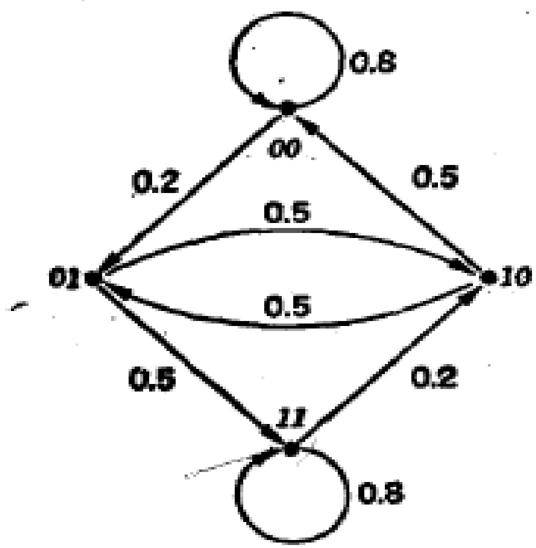


FIG. 2-4. Diagrama de estados de una fuente de Markov de segundo orden.

Consideremos un código instantáneo con un alfabeto fuente

$$S = \{s_1, s_2, \ldots, s_q\}$$

y un alfabeto código $X = \{x_1, x_2, \ldots, x_r\}$. Sean $X_1, X_2, \ldots, X_q$ las palabras del código y, por definición, l_i la longitud (es decir, el número de símbolos del código) de la palabra X_i. Normalmente es interesante que las longitudes de las palabras del código sean lo más cortas posible. La condición necesaria y suficiente para que exista un código instantáneo con palabras de longitud $l_1, l_2, \ldots, l_q$, viene definida por la *inecuación de Kraft* (Kraft, 1949).

> La condición necesaria y suficiente para la existencia de un código instantáneo de longitudes $l_1, l_2, \ldots, l_q$ es que
>
> $$\sum_{i=1}^{q} r^{-l_i} \leq 1$$
>
> donde r es el número de símbolos diferentes que constituyen el alfabeto código.

En el caso de alfabeto binario, la inecuación de Kraft se transforma en

$$\sum_{i=1}^{q} 2^{-l_i} \leq 1 \tag{3-3}$$

donde la suma se extiende a todas las palabras del código bloque. Antes de probar esta inecuación, es interesante ver en qué forma puede