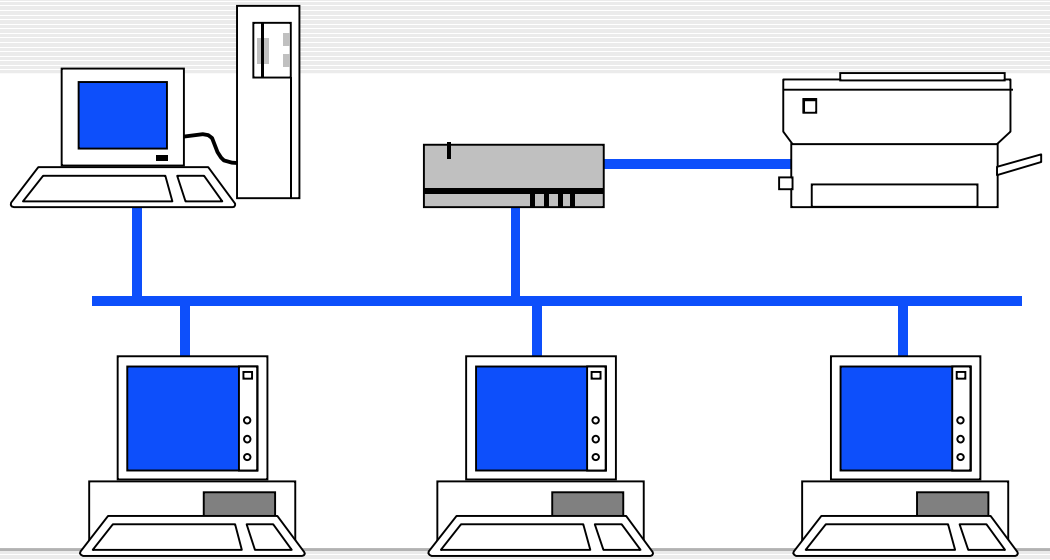
Redes de Computadores

Capa de Aplicación

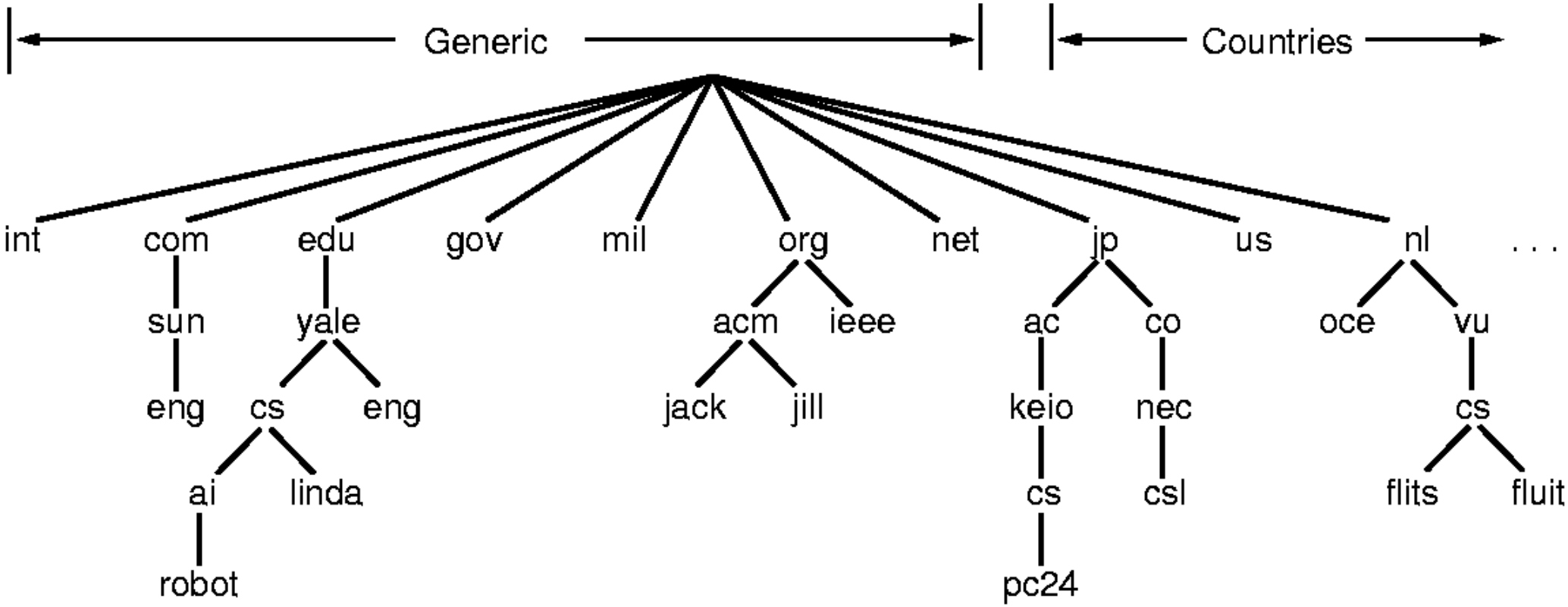


Protocolos de Capa Aplicación

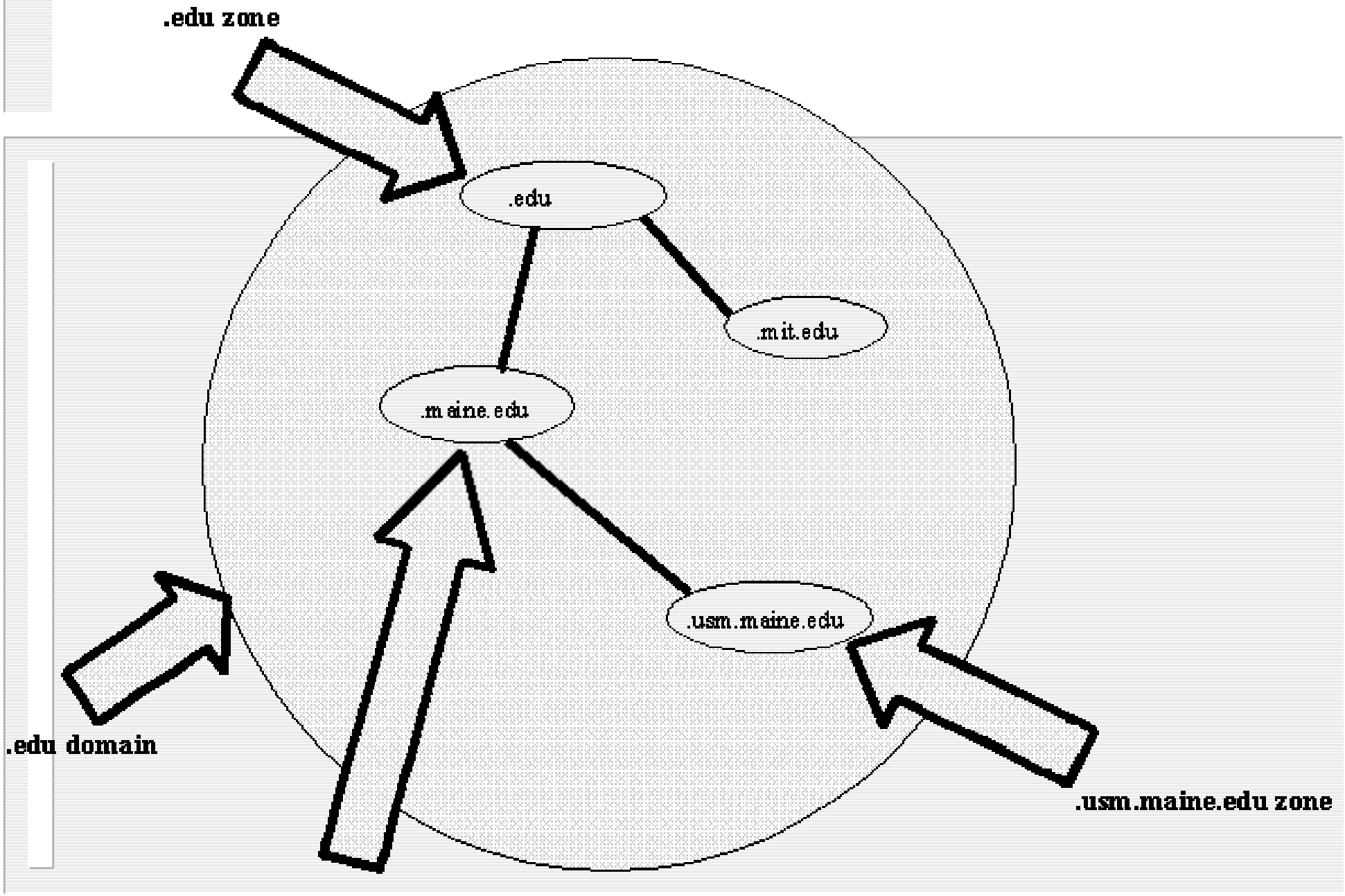
- Domain Name System (DNS)
- File Transfer Protocol (FTP)
- Correo Electrónico (SMTP)
- Smileys ;)
- USENET News (NNTP)
- Gopher
- WWW - World Wide Web (HTTP)
- Simple Network Management Protocol (SNMP, SNMPv2, RMON)
- Seguridad

DNS

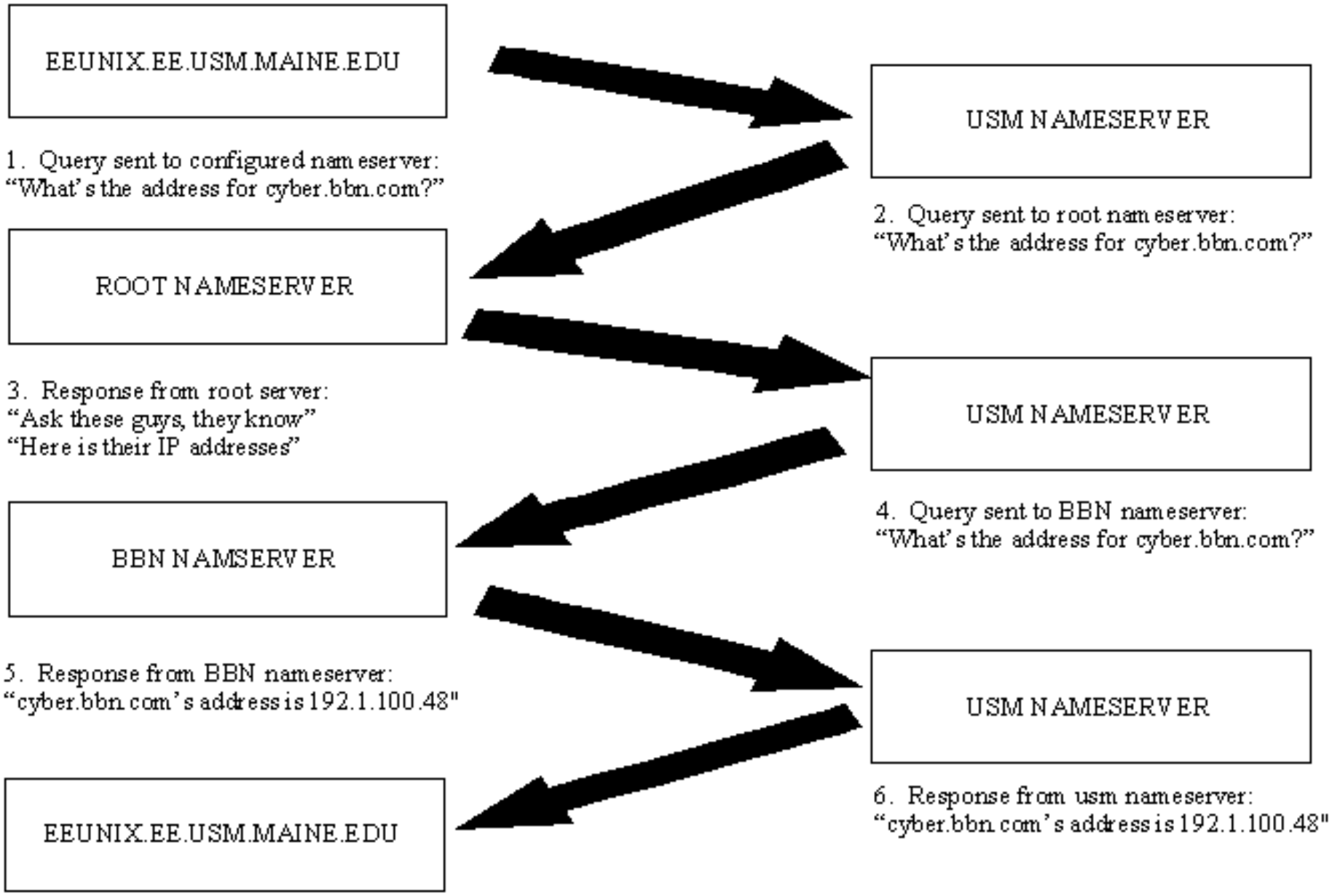
- Servicio que traduce nombres a direcciones IP y vice-versa
- Existen Servidores y Clientes DNS



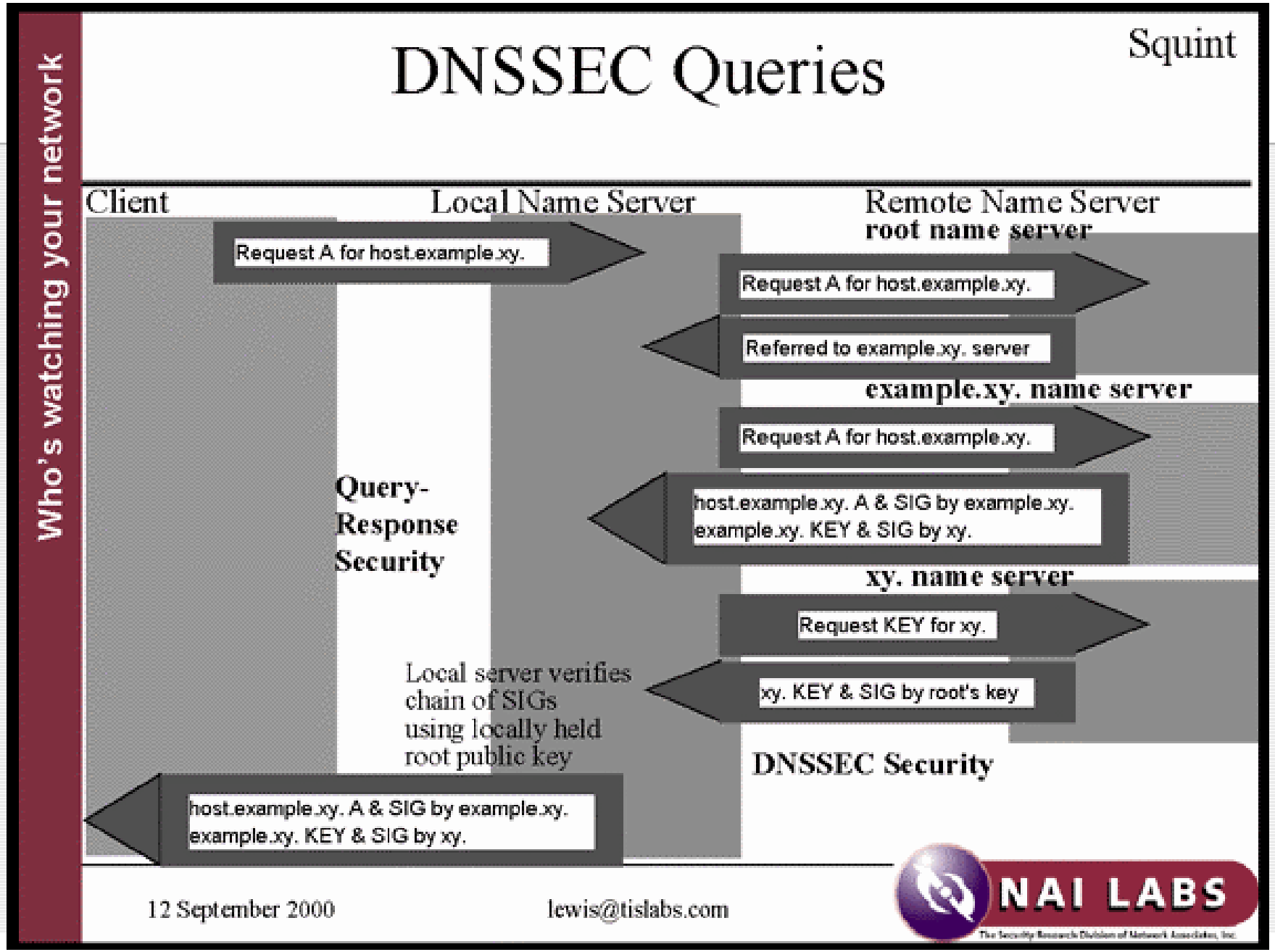
DNS


.edu zone
.edu
.mit.edu
.maine.edu
.usm.maine.edu
.edu domain
.usm.maine.edu zone
.maine.edu zone

DNS


EEUNIX.EE.USM.MAINE.EDU
USM NAMESERVER
1. Query sent to configured nameserver:
"What's the address for cyber.bbn.com?"
2. Query sent to root nameserver:
"What's the address for cyber.bbn.com?"
ROOT NAMESERVER
USM NAMESERVER
3. Response from root server:
"Ask these guys, they know"
"Here is their IP addresses"
4. Query sent to BBN nameserver:
"What's the address for cyber.bbn.com?"
BBN NAMSERVER
USM NAMESERVER
5. Response from BBN nameserver:
"cyber.bbn.com's address is 192.1.100.48"
6. Response from usm nameserver:
"cyber.bbn.com's address is 192.1.100.48"
EEUNIX.EE.USM.MAINE.EDU

DNS SEC


Who's watching your network
DNSSEC Queries
Squint
Client
Local Name Server
Remote Name Server
root name server
Request A for host.example.xy.
Request A for host.example.xy.
Referred to example.xy. server
example.xy. name server
Request A for host.example.xy.
host.example.xy. A & SIG by example.xy.
example.xy. KEY & SIG by xy.
Query-
Response
Security
xy. name server
Request KEY for xy.
xy. KEY & SIG by root's key
Local server verifies
chain of SIGs
using locally held
root public key
DNSSEC Security
host.example.xy. A & SIG by example.xy.
example.xy. KEY & SIG by xy.
12 September 2000
lewis@tislabs.com
NAI LABS

DNS

- Campos de una zona en un servidor DNS

Type	Meaning	Value
SOA	Start of Authority	Parameters for this zone
A	IP address of a host	32-Bit integer
MX	Mail exchange	Priority, domain willing to accept email
NS	Name Server	Name of a server for this domain
CNAME	Canonical name	Domain name
PTR	Pointer	Alias for an IP address
HINFO	Host description	CPU and OS in ASCII
TXT	Text	Uninterpreted ASCII text

DNS

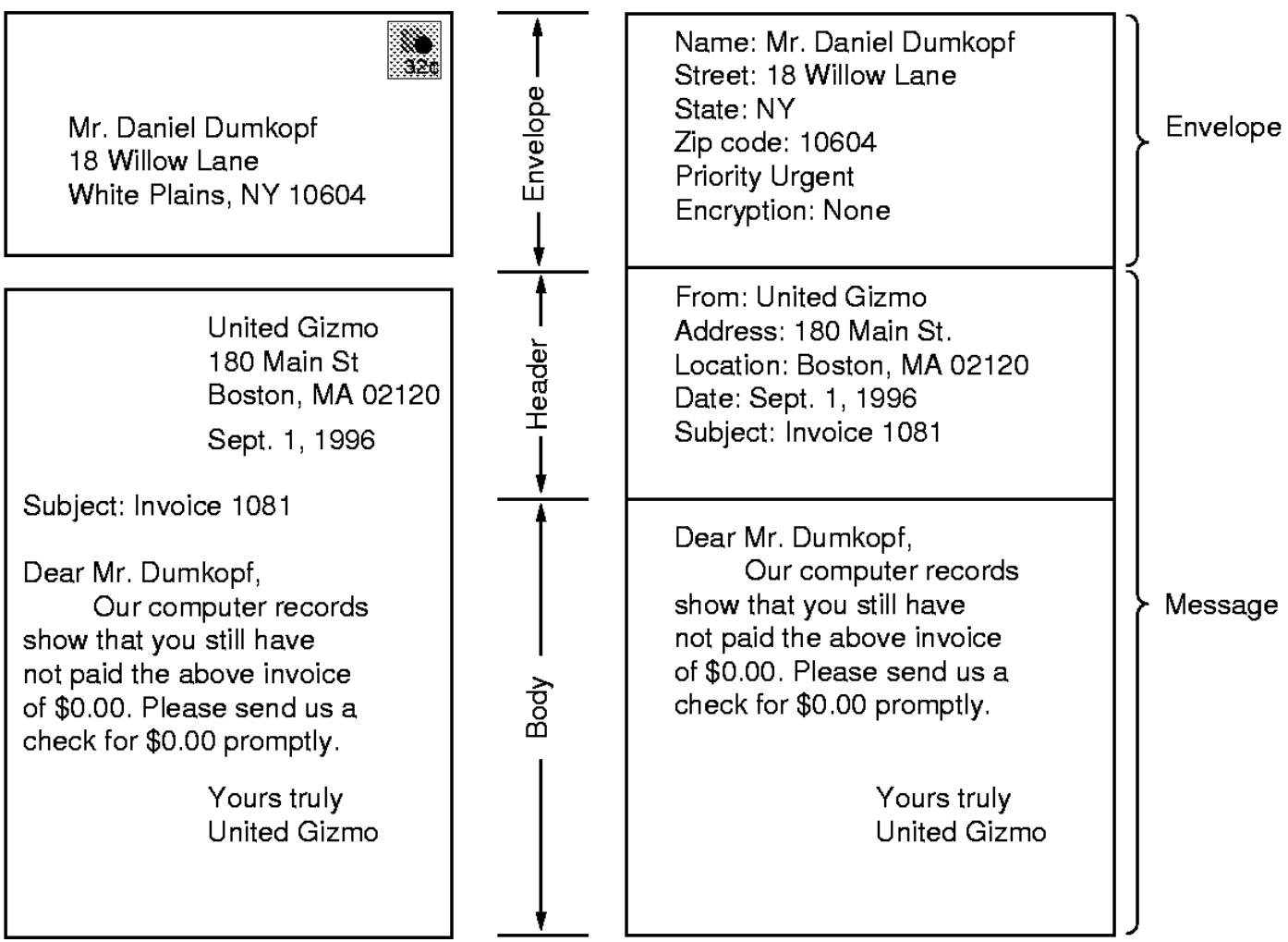
```
; alumnos.utfsm.cl
; servidores de alumnos
;
$TTL 86400      ; 1 dia
$ORIGIN alumnos.utfsm.cl.

@               IN      SOA     huasco.dcsc.utfsm.cl.   hostmaster.dcsc.utfsm.cl. (
                        2001060501      ; Serial
                        10800           ; Refresh       3 horas
                        1800            ; Retry         30 min
                        604800          ; Expire        1 semana
                        86400   )       ; Minimum       1 dia
                IN      NS      huasco.dcsc.utfsm.cl.
                IN      NS      lauca.alumnos.utfsm.cl.
;;; Mail exchangers

@               IN      MX  40  lauca.alumnos.utfsm.cl.
                IN      MX  90  rapel.dcsc.utfsm.cl.
mailhost        IN      CNAME   lauca.alumnos.utfsm.cl.
www             IN      CNAME   lauca.alumnos.utfsm.cl.
webmail         IN      CNAME   lauca.alumnos.utfsm.cl.

;;; Machines

loa             IN      A       146.83.198.9            ; sun ultra2
                IN      MX      20 lauca.alumnos.utfsm.cl.
                IN      MX      40 rapel.dcsc.utfsm.cl.


etc......
```

FTP

- Primera aplicación conceptualmente en crearse
- Consiste en transferir archivos desde un computador o máquina a otro
- No es tan simple como parece....
  - Archivos binarios y texto (ASCII o EBCDIC)
  - Little o Big Endian
  - Permisos de lectura / escritura distintos en diferentes máquinas
  - FAT, NTFS, CDFS, UFS, etc...
  - case sensitive (HoLa.txt != HOLA.txt)
  - entrega CONFIABLE del archivo
- El email es una transferencia de archivos.....

Email

- Es la aplicación de Red más usada.



Email

Headers (Encabezados) de un email

Header	Meaning
To:	Email address(es) of primary recipient(s)
Cc:	Email address(es) of secondary recipient(s)
Bcc:	Email address(es) for blind carbon copies
From:	Person or people who created the message
Sender:	Email address of the actual sender
Received:	Line added by each transfer agent along the route
Return-Path:	Can be used to identify a path back to the sender

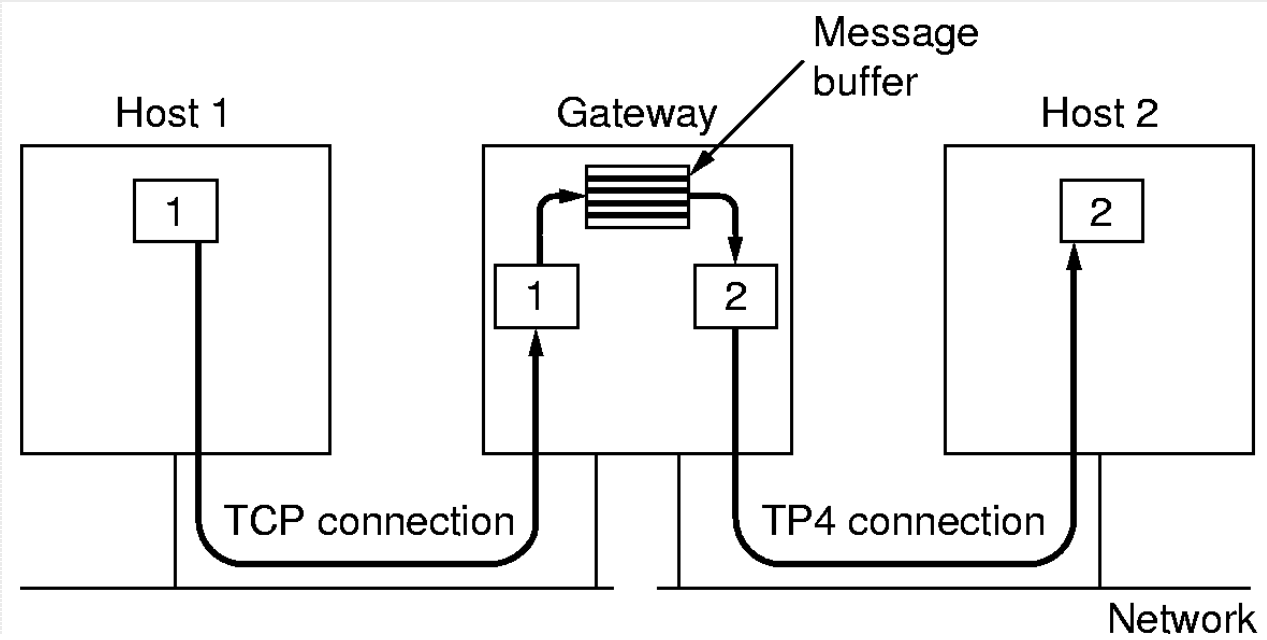
Email

Headers del email

Header	Meaning
Date:	The date and time the message was sent
Reply-To:	Email address to which replies should be sent
Message-Id:	Unique number for referencing this message later
In-Reply-To:	Message-Id of the message to which this is a reply
References:	Other relevant Message-Ids
Keywords:	User chosen keywords
Subject:	Short summary of the message for the one-line display

Email

- Existen Gateways de Email (traducción, revisión, filtraje, etc)
- Protocolo entre:
  - Cliente y Servidor Email : POP3, IMAP (consultar casilla email)
  - Servidor y Servidor: SMTP (Simple Mail Transfer Protocol)



Smileys

- Forma de agregar *sentimiento* a una frase, dado que aplicaciones antiguas sólo TX código ASCII en los email.
- Aplicaciones moderna ahora poseen iconos para este fin.

Smiley	Meaning	Smiley	Meaning	Smiley	Meaning
:-)	I'm happy	=|:-)	Abe Lincoln	:+)	Big nose
:-(	I'm sad/angry	=):-)	Uncle Sam	:-))	Double chin
:-|	I'm apathetic	*<:-)	Santa Claus	:-{)	Mustache
;-)	I'm winking	<:-(	Dunce	#:-)	Matted hair
:-(O)	I'm yelling	(-:	Australian	8-)	Wears glasses
:-(*)	I'm vomiting	:-)X	Man with bowtie	C:-)	Large brain

USENET News

- Consiste en la “publicación” de mensajes tipo email
- Existen jerarquías de acuerdo al tema de discusión.

Name	Topics covered
Comp	Computers, computer science, and the computer industry
Sci	The physical sciences and engineering
Humanities	Literature and the humanities
News	Discussion of USENET itself
Rec	Recreational activities, including sports and music
Misc	Everything that does not fit in somewhere else
Soc	Socializing and social issues
Talk	Diatribes, polemics, debates and arguments galore
Alt	Alternative tree covering virtually everything

USENET News

Mapa de Distribución de News a nivel Mundial

Gopher

- Aplicación que permite conectarse a un servidor gopher, que provee de información pública
- Sistema de permite navegar por varios menúes de texto y llegar a un artículo.
- Generalmente los servidores Gopher eran bibliotecas
- Se considera el “precursor” de la Web
- Aún existen servidores gopher en operación
- desde un browser pueden usar: gopher://

World Wide Web

- Por fin !!! .....Interface gráfica!
- *Hypertexto*: Texto navegable
- *Multimedia*: Varios medios: texto, audio, imagen, video.
- La WWW es un sistema de Hypermedia !!

WWW

- URL (Uniform Resource Locator) posibles....

Name	Used for	Example
http	Hypertext (HTML)	http://www.cs.vu.nl/~ast/
ftp	FTP	ftp://ftp.cs.vu.nl/pub/minix/README
file	Local file	/usr/suzanne/prog.c
news	News group	news:comp.os.minix
news	News article	news:AA0134223112@cs.utah.edu
gopher	Gopher	gopher://gopher.tc.umn.edu/11/Libraries
mailto	Sending email	mailto:kim@acm.org
telnet	Remote login	telnet://www.w3.org:80

WWW

- Pasos de la conexión
  - Browser necesita la URL http://www.utfsm.cl/index.html
  - PC pide a su servidor DNS el IP de “www.utfsm.cl”
  - DNS entrega 146.83.198.62
  - Browser se conecta a 146.83.198.62 en el port 80
  - Envía un “GET /index.html”
  - www.utfsm.cl le envía el archivo “index.html”
  - si hay imágenes, también se transfieren
  - Browser despliega el texto y despliega las imágenes de la página
  - se cierra la conexión TCP

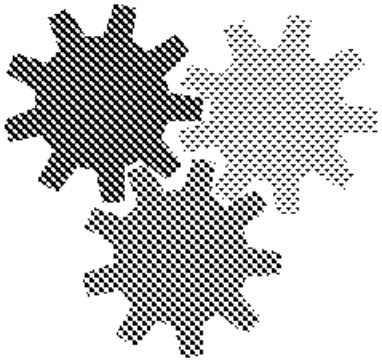
WWW

Código HTML de una página web

```
<HTML> <HEAD> <TITLE> AMALGAMATED WIDGET, INC. </TITLE> </HEAD>
<BODY> <H1> Welcome to AWI's Home Page </H1>
<IMG SRC="http://www.widget.com/images/logo.gif" ALT="AWI Logo"> <BR>
We are so happy that you have chosen to visit <B> Amalgamated Widget's</B>
home page. We hope <I> you </I> will find all the information you need here.
<P>Below we have links to information about our many fine products.
You can order electronically (by WWW), by telephone, or by fax. <HR>
<H2> Product information </H2>
<UL> <LI> <A HREF="http://widget.com/products/big">   Big widgets    </A>
        <LI> <A HREF="http://widget.com/products/little"> Little widgets </A>
</UL>
<H2> Telephone numbers </H2>
<UL> <LI> By telephone: 1-800-WIDGETS
        <LI> By fax: 1-415-765-4321
</UL> </BODY> </HTML>
```

WWW

Welcome to AWI's Home Page



We are so happy that you have chosen to visit **Amalgamated Widget's** home page. We hope *you* will find all the information you need here.

Below we have links to information about our many fine products. You can order electronically (by WWW), by telephone, or by FAX.

Product Information

- Big widgets
- Little widgets

Telephone numbers

- 1-800-WIDGETS
- 1-415-765-4321

WWW

Páginas Web Interactivas

Widget Order Form

Name

Street address

City State Country

Credit card # Expires M/C Visa

Widget size Big Little Ship by express courier

Submit order

Thank you for ordering an AWI widget, the best widget money can buy!

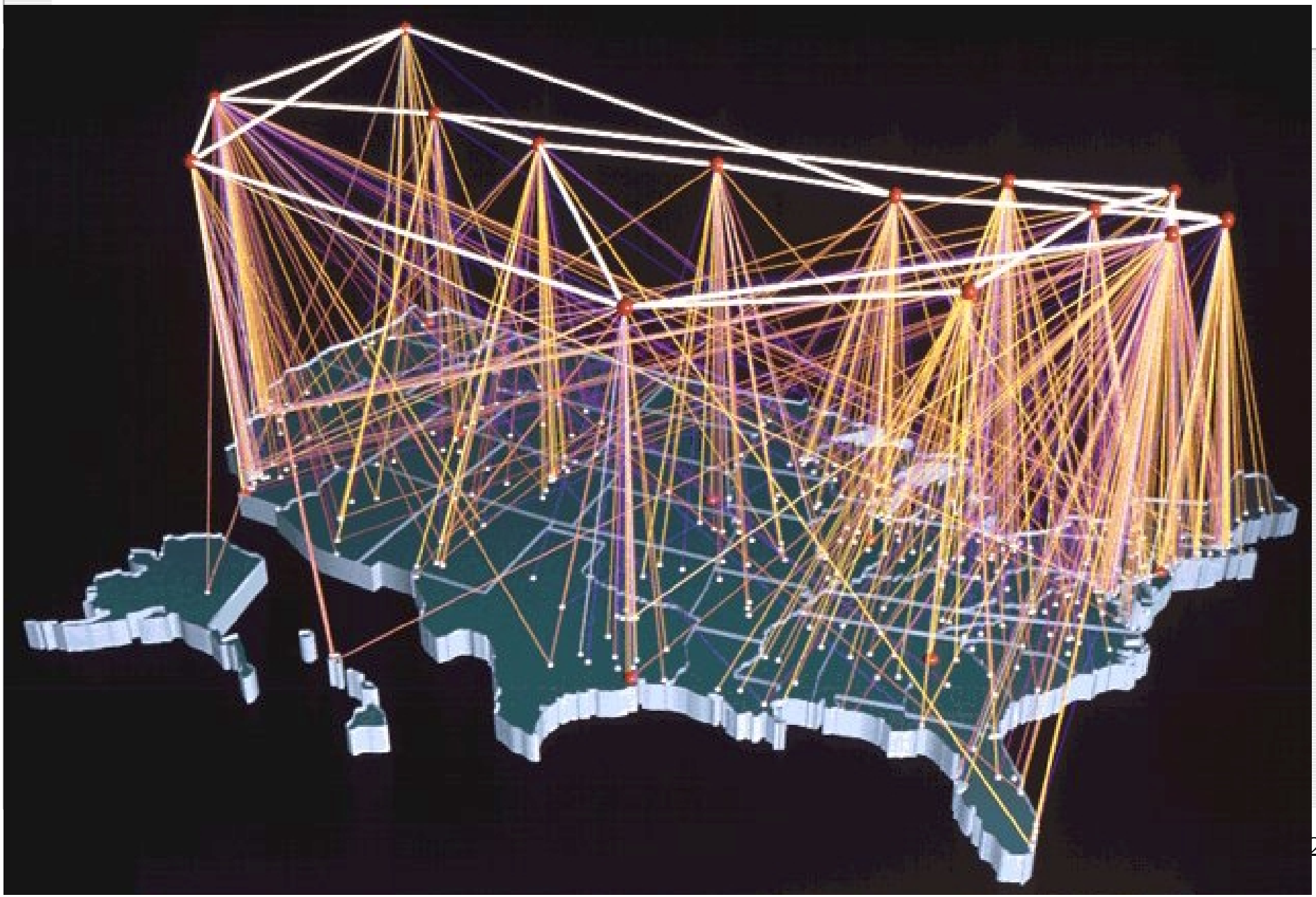
WWW

Mapas de Internet

The Atlas of Cyberspace

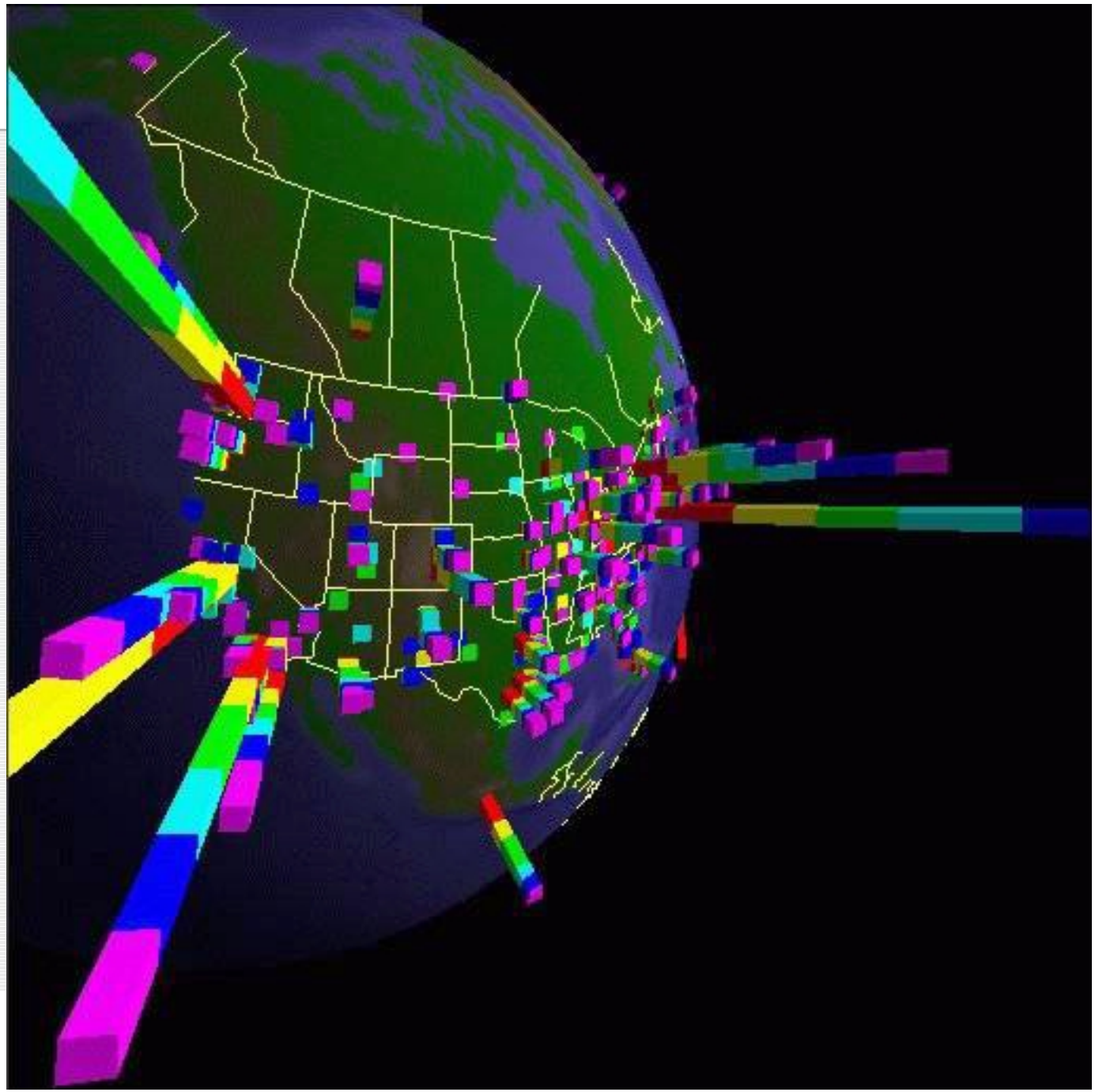
http://www.geog.ucl.ac.uk/casa/martin/atlas/atlas.html

Backbone de USA



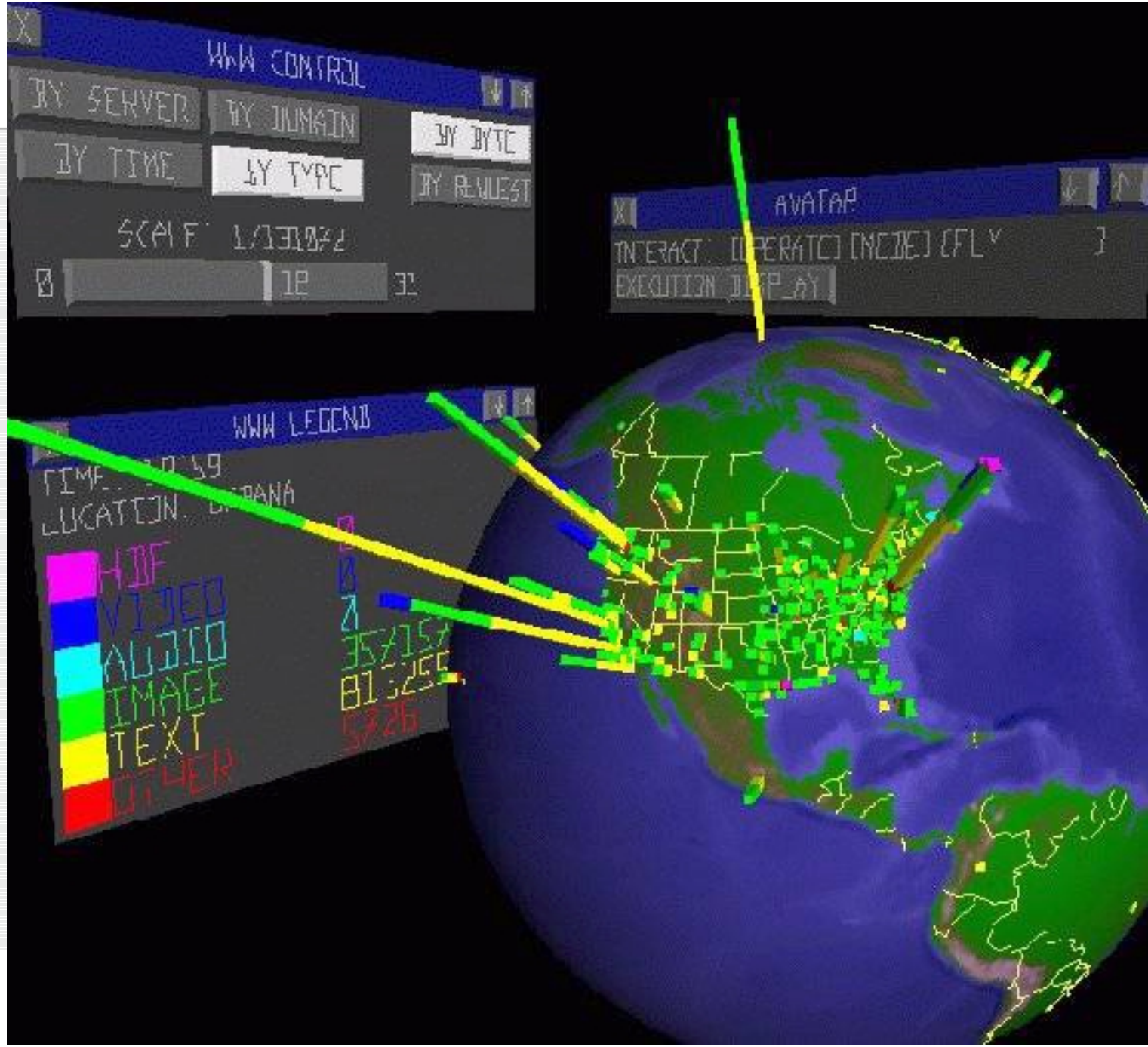
WWW

Tráfico en Tiempo Real de WWW



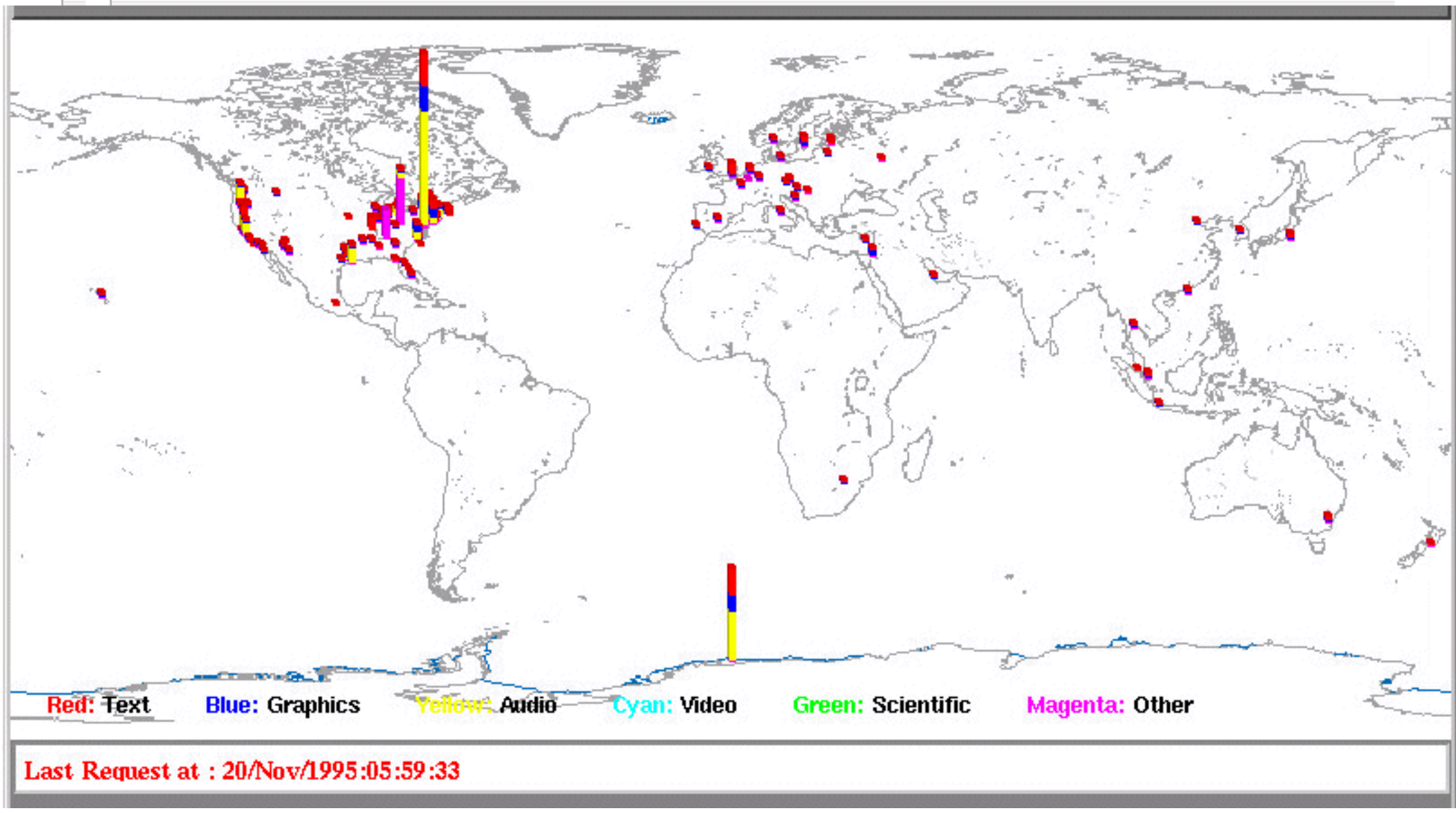
WWW

Tráfico en Tiempo Real de WWW

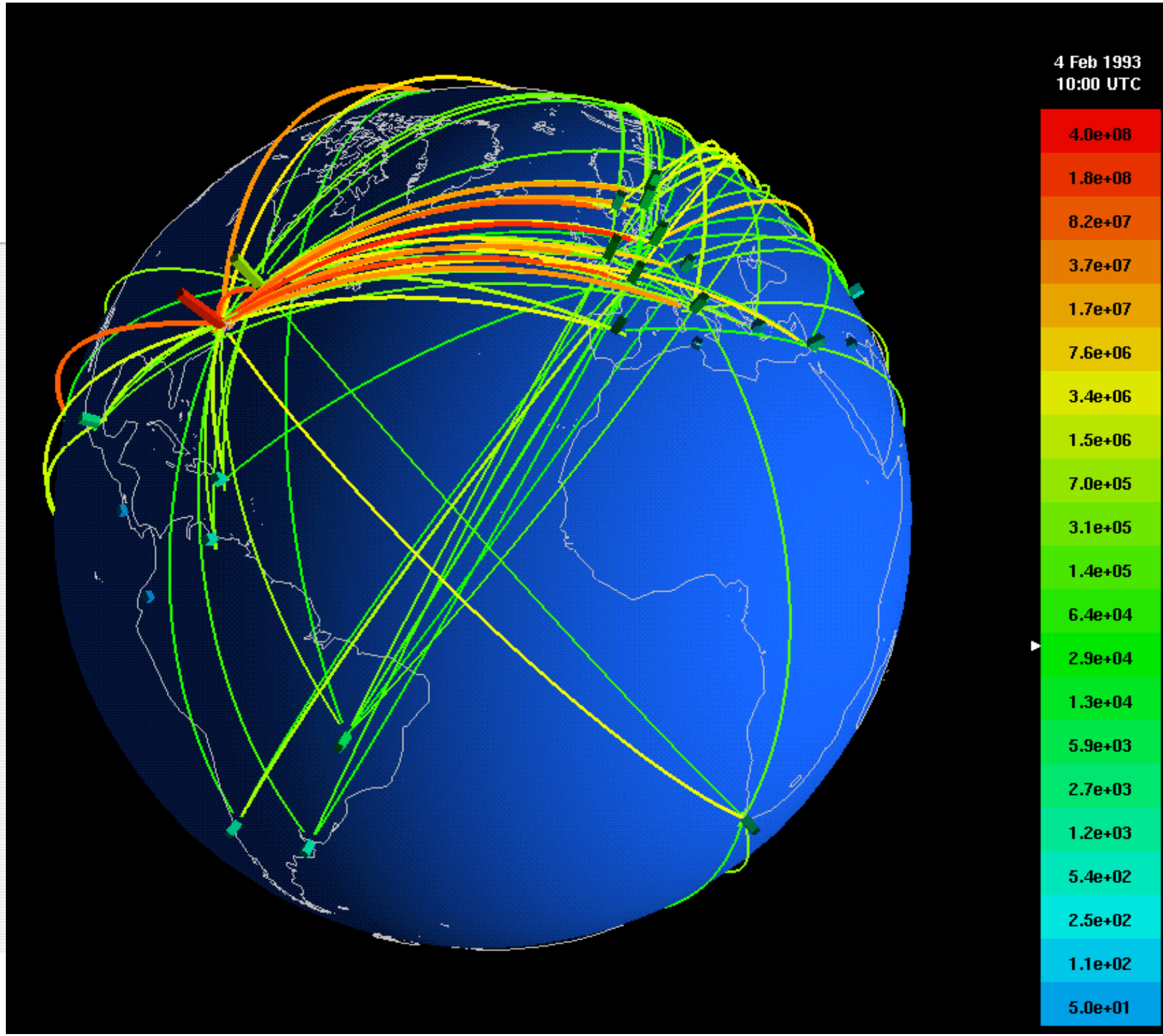


WWW

Tráfico de WWW separado por tipo

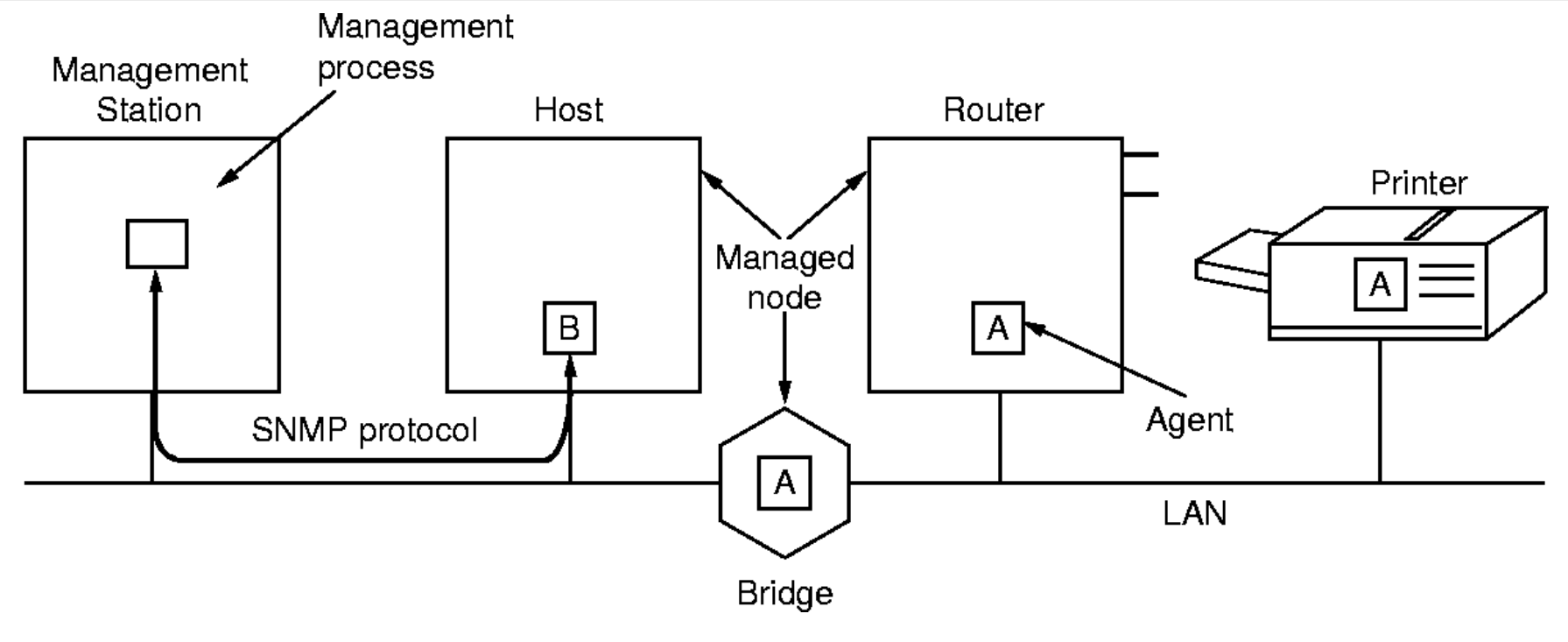


Cantidad de Tráfico de WWW



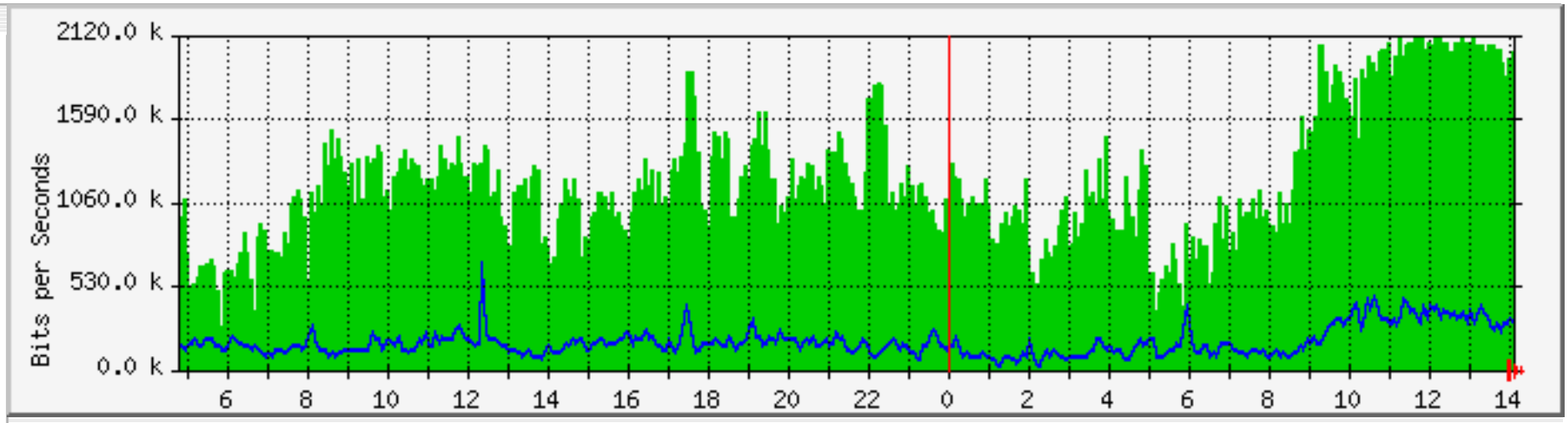
SNMP

- Protocolo de Administración de Redes
- Consiste en Agentes y Estaciones de Administración.

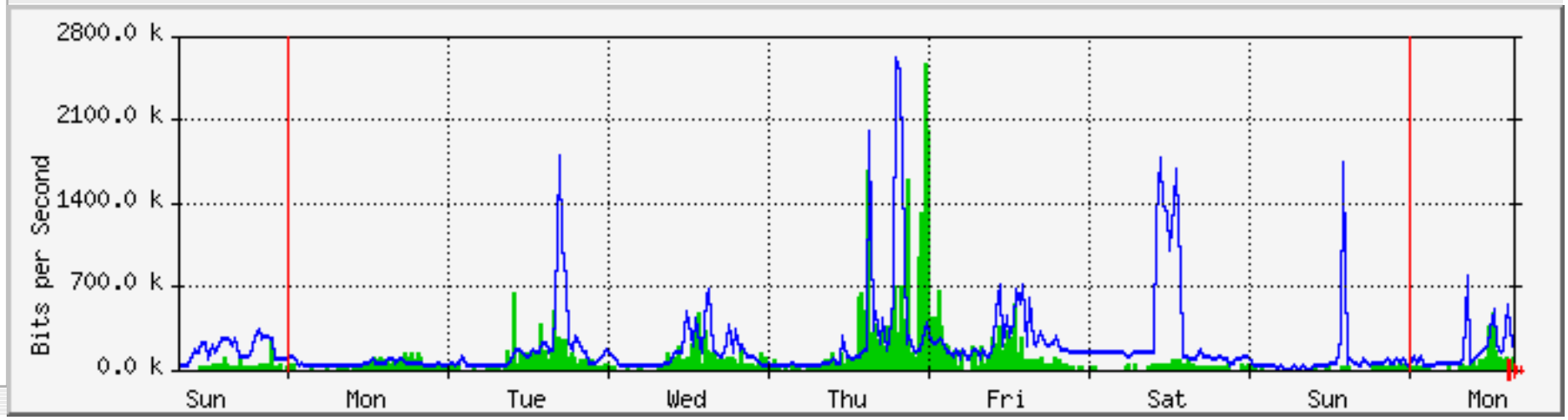


SNMP

Trafico UTFSM

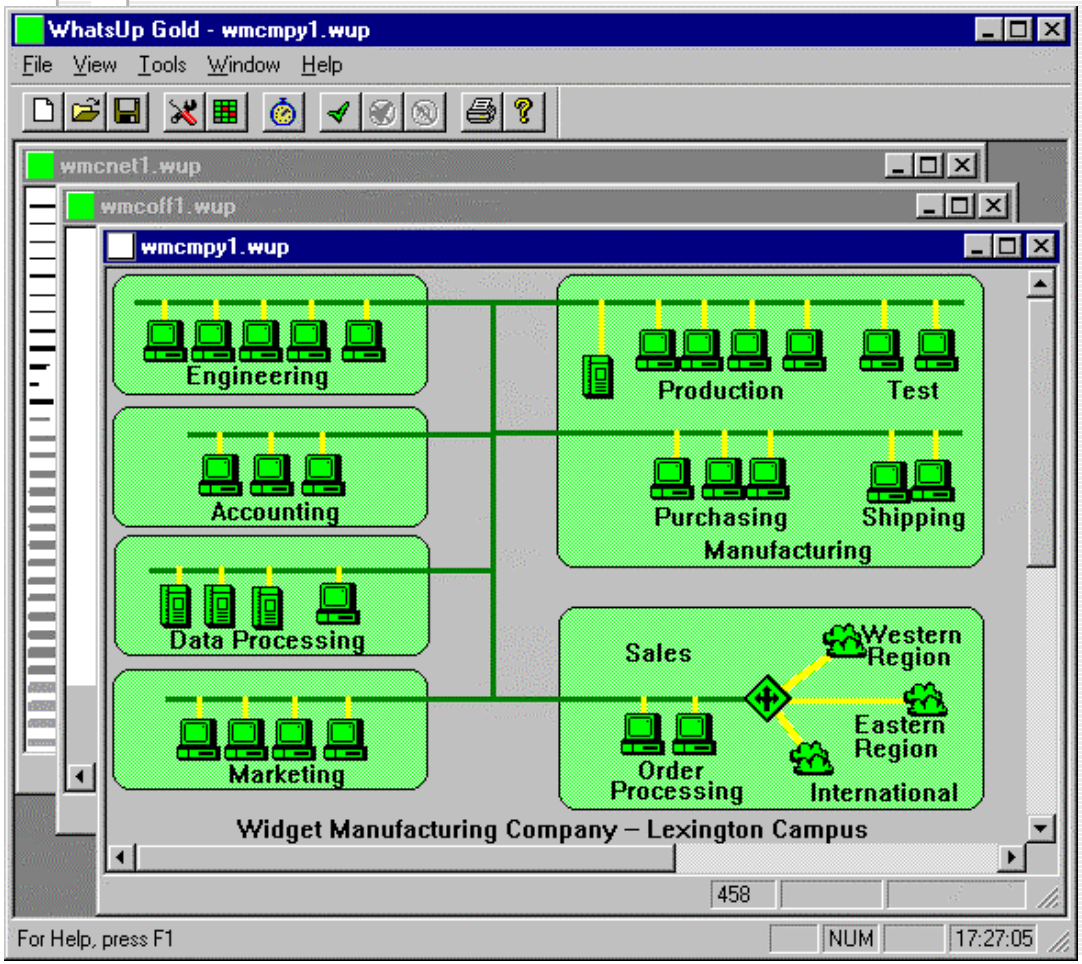


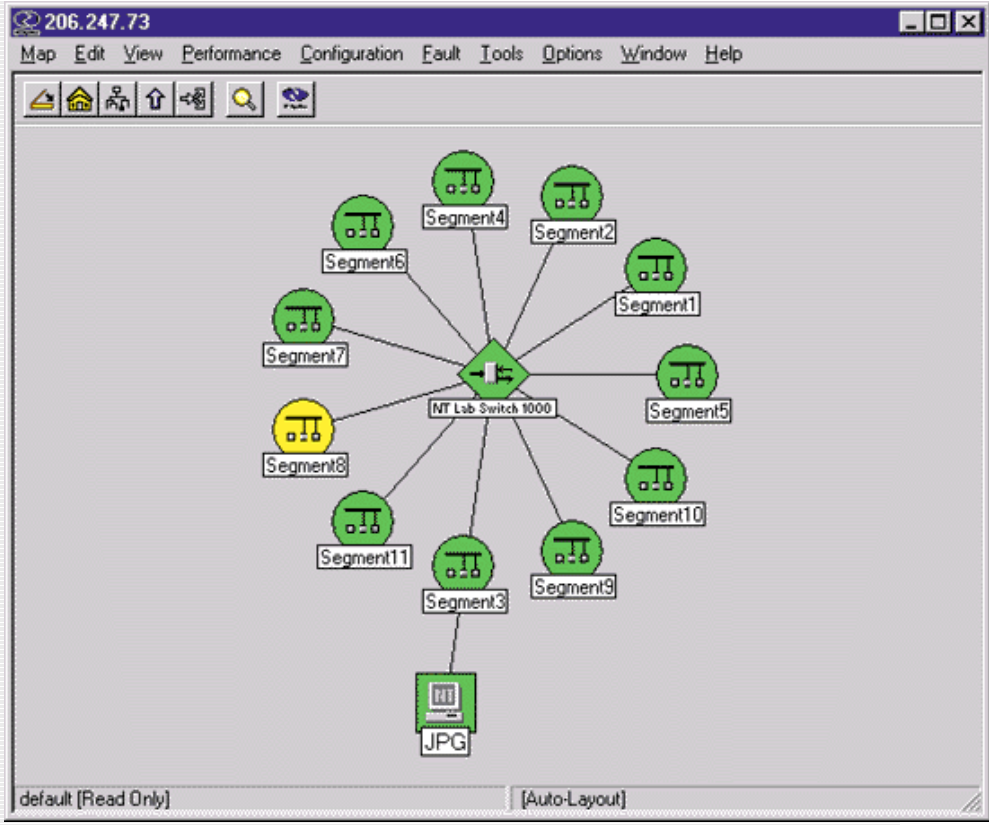
Trafico Depto Electrónica



SNMP

Aplicaciones SNMP





Seguridad - Preguntas Claves

- ¿Está ud. siempre seguro de la identidad de la persona con que realiza conversación por la red ?
- ¿ Enviaría Ud. información confidencial/sensible como su # tarjeta de crédito a través de Internet, aunque confíe en el otro extremo ?
- ¿ Está Ud. seguro de que su mensaje no fue alterado en el camino ?
- ¿ Está preocupado que su contraparte puede negar un compromiso u orden recibida a través de Internet ?
- ¿ Desea darle un efecto legal a sus transacciones electrónicas ?

Seguridad - Perfiles

Adversary	Goal
Student	To have fun snooping on people's email
Hacker	To test out someone's security system; steal data
Sales rep	To claim to represent all of Europe, not just Andorra
Businessman	To discover a competitor's strategic marketing plan
Ex-employee	To get revenge for being fired
Accountant	To embezzle money from a company
Stockbroker	To deny a promise made to a customer by email
Con man	To steal credit card numbers for sale
Spy	To learn an enemy's military strength
Terrorist	To steal germ warfare secrets

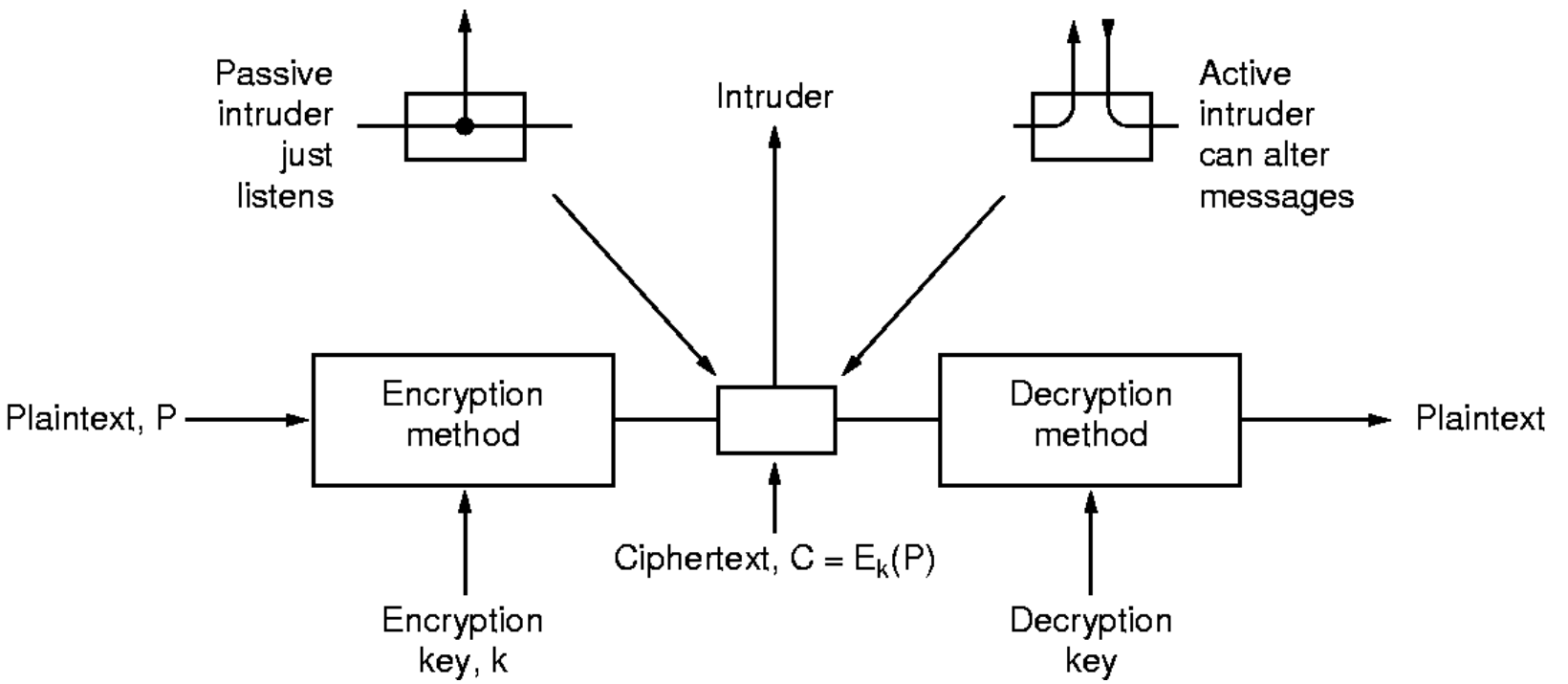
Seguridad - Soluciones

- Autentificación
  - saber realmente quién es la persona con que se está comunicando
- Confidencialidad
  - el mensaje no puede ser leído por una persona no autorizada
- Integridad
  - el mensaje no puede ser cambiado sin ser detectado
- No - Repudio
  - la transacción no puede ser negada por la contraparte

Seguridad

- Cifrar - Encriptar la data
- Uso de una llave para encriptar (Criptografía Simétrica)

$$D_K(E_K(P)) = P$$



Seguridad

Cifrado por Sustitución (C. Simétrica)

texto: **a b c d e f g h i j k l m n o p q r s t u v w x y z**
ciphertext: **Q W E R T Y U I O P A S D F G H J K L Z X C V B N M**

- Mensaje original
  - “hola” ==> Mensaje cifrado “OHDQ”
- Sistema usado por Julio César.....

Seguridad

Cifrado por Transposición (C. Simétrica)

M	E	G	A	B	U	C	K
7	4	5	1	2	8	3	6
p	l	e	a	s	e	t	r
a	n	s	f	e	r	o	n
e	m	i	l	l	i	o	n
d	o	l	l	a	r	s	t
o	m	y	s	w	i	s	s
b	a	n	k	a	c	c	o
u	n	t	s	i	x	t	w
o	t	w	o	a	b	c	d

Plaintext

pleasetransferonemilliondollarsto
myswissbankaccountsixtwotwo

Ciphertext

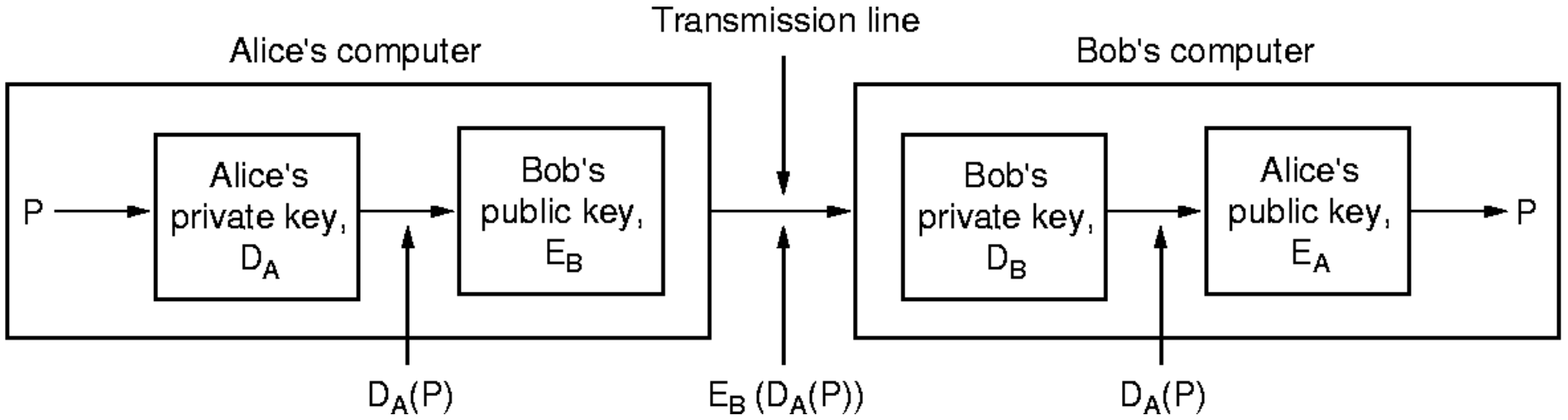
AFLLSKSOSELAWAIATOOSSCTCLNMOMANT
ESILYNTWRNNTSOWDPAEDOBUOERIRICXB

Seguridad - Soluciones

- Criptografía Simétrica
  - Una llave para “confidencialidad”
  - Desventajas
    - Debe intercambiarse la llave en forma segura (?)
    - No existe autentificación
    - No existe no-repudio
- Criptografía Asimétrica (Public Key Criptography)
  - Cada usuario posee una llave privada y una llave pública
  - lo que se encripta con una llave puede desencriptarse con la otra
  - la llave privada es mantenida en secreto por el usuario
  - la llave pública es conocida por el resto de la comunidad
  - una llave no puede ser deducida teniendo la otra.

Seguridad

Criptografía Asimétrica (Public Key Criptography)



Sólo Bob puede leer el mensaje (confidencialidad)

Sólo Alice puede haber generado el mensaje (autentificación)

Seguridad

- Problemas....
  - Algoritmo de Criptografía Asimétrica es computacionalmente más intenso en recursos que un Algoritmo de Criptografía Simétrica
  - Y.....¿Cómo sabe Alice que la llave pública de Bob que está usando es la correcta? (E_B es realmente la llave pública de Bob?)
  - Existe necesidad de que un mensaje pueda ser autentificado, pero no necesariamente debe ser cifrado
  - ¿ Qué pasa con el no-repudio ?
- *Solución: FIRMA DIGITAL y CERTIFICADO DIGITAL*

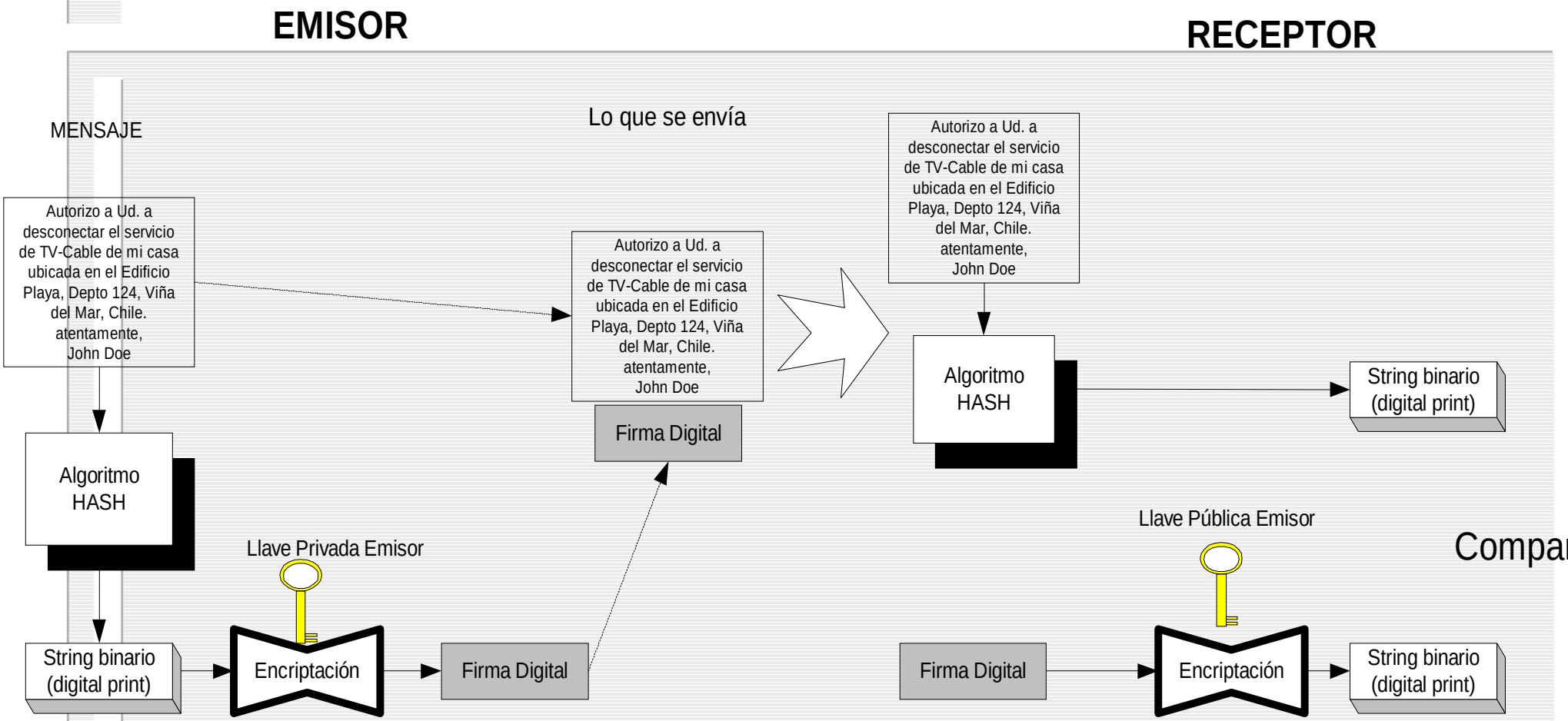
FIRMA DIGITAL

- Alicia desea enviar un email firmado a BOB
  - Autentificación
  - Encriptación es opcional
- Alicia somete el mensaje a un algoritmo HASH (SHA-1 u otro) que arroja un string binario de tamaño fijo (digital print)
- Alicia encripta este string con su llave privada, obteniendo la *firma digital*
- Alicia envía el mensaje (con/sin cifrar) junto con la firma digital

FIRMA DIGITAL

- Bob recibe el mensaje y la firma digital
- Bob decripta la firma digital con la llave pública de Alicia, obteniendo un string binario
- Bob somete el mensaje al mismo algoritmo HASH y obtiene un string binario
- Si ambos strings binarios son iguales, implica que:
  - SOLO Alicia pudo haber generado el mensaje (*autentificación*)
  - El mensaje no fue modificado en el camino (*integridad*)
  - Si Bob alguna vez responde, entonces no podrá negar que recibió este mensaje (*no-repudio*)
  - La encriptación al mensaje sólo se aplica si se desea *confidencialidad*.

Firma Digital



Pero aún persiste....¿Cómo sabe el Receptor que la Llave pública es realmente del emisor?

Certificado Digital

- El usuario deberá generar su par llave privada/pública en su PC
- Luego se contacta con una Autoridad Certificadora (CA) reconocida y les envía su llave pública junto con acreditación personal (licencia de conducir u otro) y presentarse personalmente en una Autoridad Registradora de esa CA (Clase 3)
- La CA verifica los datos y genera un certificado que se le devuelve al usuario
- El certificado es un archivo que contiene la llave pública y datos del usuario, todo firmado digitalmente con la llave privada de la CA
- La llave pública del CA está integrada a los browsers y lectores de email
- En cada mensaje, el usuario envía el mensaje, la firma digital y su certificado
- Con ello, otro usuario puede estar seguro que la llave pública en cuestión corresponde al usuario en cuestión.

Firma y CertificadoDigital