Aplicaciones y Servicios en Redes

Tema 02. Aplicaciones y Servicios Distribuidos

Alberto Eloy García Gutiérrez

Luis Sánchez González

DPTO. DE INGENIERÍA DE COMUNICACIONES

Servicio de Nombres de Dominio

- Las direcciones IP no son tan fáciles de recordar como los **nombres** → asociar (nombre, dirección IP)
- Antiguamente se utilizaba el fichero **"/etc/hosts",** que estaba centralizado en un servidor con la relación de todos los nombres de forma exhaustiva y para utilizarlo, se realizaban periódicamente copias a los servidores locales.
- **Inconvenientes:** el manejo de "/etc/hosts" es un procedimiento **poco escalable**, genera mucho tráfico en el servidor, inconsistente con las copias locales y con facilidad aparecían nombres duplicados

Servicio de Nombres de Dominio

- El **servicio de nombres de dominio** se basa en un esquema jerárquico que permite asignar nombres, basándose en el concepto de *dominio*, utilizando para su gestión una *base de datos (BBDD) distribuida*. Adaptado en 1983.
- Las **consultas al DNS** son realizadas por los *clientes* a través de las rutinas de resolución ("*resolver*" o *resolvedor o resolutor, según algunas traducciones*). Estas funciones son llamadas en cada *host* desde las *aplicaciones de red*.
- Las **funciones "resolver"** sirven para hacer peticiones e interpretan las respuestas de los servidores de nombres de dominio de Internet.

DNS: Domain Name System

- Implementa la jerarquía de nombres
- Basado en:
  - Una sintaxis para los nombres y unas reglas de delegación de autoridad
  - Un sistema de computación distribuido que relaciona nombres y direcciones
- Ventajas
  - *Desaparece la carga excesiva:* la información esta distribuida por toda la red
  - *No hay Duplicidad de Nombres:* los dominios están controlados por un único administrador (*Pueden existir nombres iguales pero en dominios diferentes)*
  - *Consistencia de la Información:* está distribuida y es actualizada automáticamente sin intervención de ningún administrador.

DNS: Nombres de Dominio

- Nombre de dominio = tira de menos de 255 caracteres, formada por etiquetas separadas por puntos (cada etiqueta inferior a 63 caracteres RFC 1034) de forma jerárquica o por niveles (comenzando el nivel superior por la derecha). Cada dominio es un índice en la BBDD del DNS.
- un sufijo de nombre de dominio también es un nombre de Dominio

sol.tlmat.unican.es

sol.tlmat.unican.es ⇒ nombre de dominio de un computador
tlmat.unican.es ⇒ nombre de dominio del grupo de telemática
unican.es ⇒ nombre de dominio de la UC
es ⇒ nombre de dominio de España

- No se distinguen mayúsculas de minúsculas. Esto no se aplica a la parte izquierda de @ en las direcciones de correo.

DNS: Dominios de primer nivel

Por organización

com	organización comercial
edu	institución educativa USA
net	org. relacionada con la red
gov	org. gubernamental USA
…	…
org	otras organizaciones

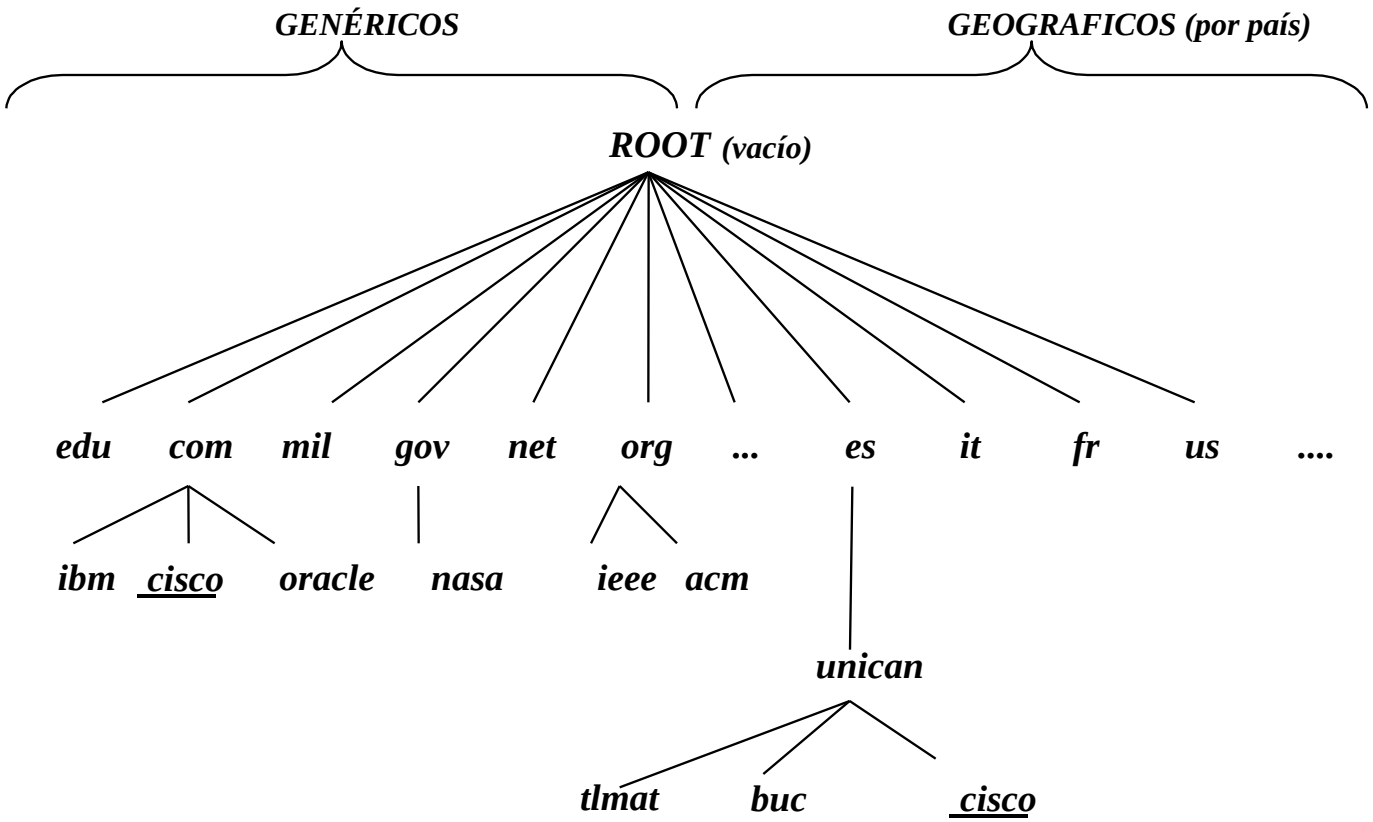
Geográfico (Códigos de dos letras ISO3166-1)

es	España
uk	Reino Unido
fr	Francia
...	Otros paises

ICANN (Internet Corporation for Assigned Names and Numbers) aprobó, (16-11-00), siete nuevos dominios de primer nivel:

aero	industria de transporte aéreo
biz	negocios
coop	Coop. sin animo de lucro
info	uso no restringido
museum	museos
name	para registro de individuos
pro	médicos, abogados ...

DNS: Jerarquía de Nombres de Dominio



DNS: Delegación de Autoridad

- La organización que posee un nombre de dominio, es responsable del funcionamiento y mantenimiento de los servidores de nombres. Este área de influencia se llama zona de autoridad

  sol.tlmat.unican.es

  - El nombre Sol ha sido aprobado por el grupo de telemática
  - El nombre tlmat ha sido aprobado por la Universidad de Cantabria
  - El nombre unican ha sido aprobado por la autoridad de Internet en España (ES-NIC)
  - El nombre es ha sido aprobado por la autoridad central de Internet

- Un domino/subdominio (dominio de nivel inferior) no tiene porque corresponder con una red/subred IP, ni tampoco una correspondencia geográfica

DNS: Registro de Dominios

- Para registrar un nombre en Internet, se solicita un nombre bajo uno de los dominios de primer nivel
  - Ejemplo:

    churreria.es

    bunyuelos.com
- Luego, la empresa solicitante puede nombrar sus máquinas como estime conveniente (introduciendo una nueva jerarquía o no):

  porras.madrid.**churreria.es**

  calabaza.**bunyuelos.com**
- En España:
  - Dominios **.com .org .net** (compañias acreditadas por ICANN)
    - Interdomain, S.A. www.interdomain.org
    - Nominalia Internet S.L www.nominalia.com

    (unos 34 euros por año)
  - Dominio **.es**
    - ES-NIC: www.nic.es

    (unos 80 - 210 euros el alta y 56 - 100 euros por año)

Coste de Dominios Internet (año 2012)

Precios sin IVA

Dominio	Numero de años 1	2	3	4	5	6	7	8	9	10
.COM	9,00	17,50	25,80	34,00	41,25	48,00	56,00	64,00	72,00	75,00
.NET	9,00	17,50	25,80	34,00	41,25	48,00	56,00	64,00	72,00	75,00
.ORG	9,00	17,50	25,80	34,00	41,25	48,00	56,00	64,00	72,00	75,00
.CAT	25,00									
.INFO	8,00	15,00	21,00	28,00	35,00	40,50	47,25	54,00	60,75	65,00
.US	8,00	15,00	21,00	28,00	35,00	40,50	47,25	54,00	60,75	65,00
.BIZ	9,00	17,00	25,00	32,00	38,75	42,00	49,00	56,00	63,00	70,00
Precio Año	8,00	7,50	7,00	7,00	7,00	7,00	6,75	6,75	6,75	6,50
.ES	7,75	14,50	21,00	28,00	34,00					
Precio Año	7,50	7,25	7,00	7,00	6,80					
.COM.ES	2,95	5,90	8,85							
.ORG.ES	2,95	5,90	8,85							
.NOM.ES	2,95	5,90	8,85							
Precio Año	2,95	2,95	2,95							
.EU	7,00	13,00	18,75	25,00	30,00	36,00	42,00	48,00	54,00	60,00
Precio Año	7,00	6,50	6,25	6,25	6,00	6,00	6,00	6,00	6,00	6,00
.NAME	9,00	17,00	24,00	32,00	40,00	45,00	52,50	60,00	65,25	70,00
.WS	9,00	17,00	24,00	32,00	40,00	45,00	52,50	60,00	65,25	70,00
Precio año	9,00	6,50	8,00	8,00	8,00	7,50	7,50	7,50	7,50	7,00
.MOBI	12,95	25,90	37,50	50,00	62,50					
Precio Año	12,95	12,95	12,50	12,50	12,50					
.BZ	16,95	33,90	50,25	66,00	80,00					
.CC	16,95	33,90	50,25	66,00	80,00					
Precio Año	16,95	16,95	16,75	16,50	16,00					
.TV	20,95	41,90	62,25	83,00	102,50					
Precio Año	20,95	20,95	20,75	20,75	20,50					
.CO.UK		12,00	18,00							
Precio Año		6,00	6,00							
.MN	35,00	68,00	99,00	124,00	150,00					
Precio Año	35,00	34,00	33,00	31,00	30,00					
.TEL	9,95	19,60	29,25							
Precio Año	9,95	9,80	9,75							

Listado de Agentes Registradores en España

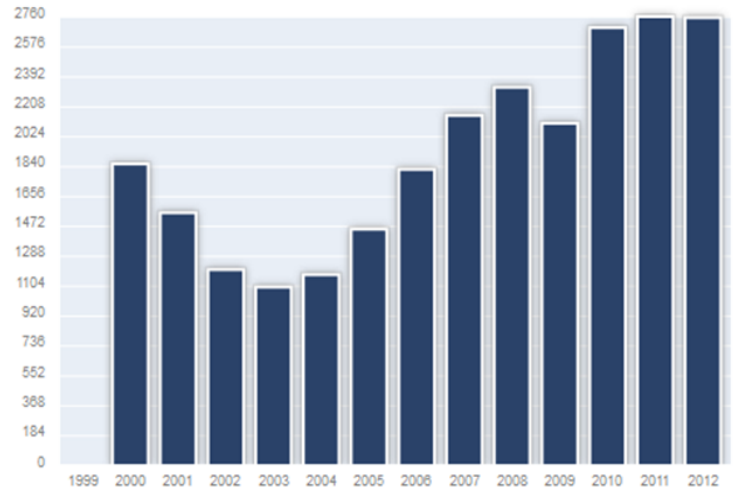
Fuente:
Dominios.es (www.nic.es)

1&1	ELZABURU	NEODIGIT
1API	ENTORNO DIGITAL	NERION NETWORKS
123 DOMAIN.EU	EPAG Domainservices	NETIM
ABANSYS	EURODNS	NETKIA
ACENS	GANDI SAS	NEXICA
ACTIVE 24	HERRERO Y ASOCIADOS	NOMINALIA
ARGORED	HISPAWEB	NOM-IQ LTD
ARRAKIS	HOSPEDAJE Y DOMINIOS	OPENPROVIDER
ARSYS	HOSTINET	OVH
ASCIO	IBERCOM	PDR
AVANZAS	IDECNET	PIENSA SOLUTIONS
AXARnet	IGARCOM	PLANETDOMAIN
BB ONLINE	IMPRESIONES WEB	PONS PATENTES Y MARCAS
CDMON	INDOM	RECOL
CENTRORED	INFORTELECOM	REDCORUNA
CHIVALGES	INSTRA CORPORATION	REALTIME REGISTER
CLARKE, MODET & CO.	INTERDOMAIN	REGISTER.ES
COMALIS	INTERDOMINIOS	SAFENAMES LTD
COMVIVE	INTERNET NAMES	SANE SYSTEMS
CONFIGBOX	INTERNETWORX	SARENET
CORE Internet Council of Registrars	INTERNETX	SCIP
CPS-DATENSYSTEME	IP MIRROR PTE. LTD.	SERDATA
CSC Corporate Domains, Inc.	IS-FUN	SERVEISWEB
DIGITAL VALUE	J.ISERN PATENTES Y MARCAS	STRATO
DIGIVAL	KEY SYSTEMS	SIOSI
DINAHOSTING	MAILCLUB	SYNC
DOCUMENTDATA ANSTALT	MARCARIA	TUCOWS
DOMAINCLUB	MARKMONITOR	TU DOMINIO
DOMAININFO	MESHDIGITAL	UBILIBET
DOMAIN PROTECT	NAMEBAY	UNITED DOMAINS
DOMIHOST	NAMESHIELD	VARIOMEDIA
DOMENESHOP	NameWeb BVBA	VIRTUALPYME
DOMESTIKA	NAME.COM	WEBFUSION
EASYNET	NEMETIC	WEIS

DNS: Controversias y disputas de Nombres

- Es frecuente en ciertos dominios la utilización de nombres controvertidos.
- Dichas controversias se resuelven en la OMPI (organismo encargado de solucionar de forma amistosa estas situaciones) a nivel mundial. El procedimiento no amistoso es resuelto por los tribunales.
- A nivel anecdótico, en el año 2000, hubieron unas 2000 quejas, 100 de ellas por demandantes españoles.
- España era el tercer país en conflictos de este tipo, detrás de EEUU y UK.

Número de casos en el mundo

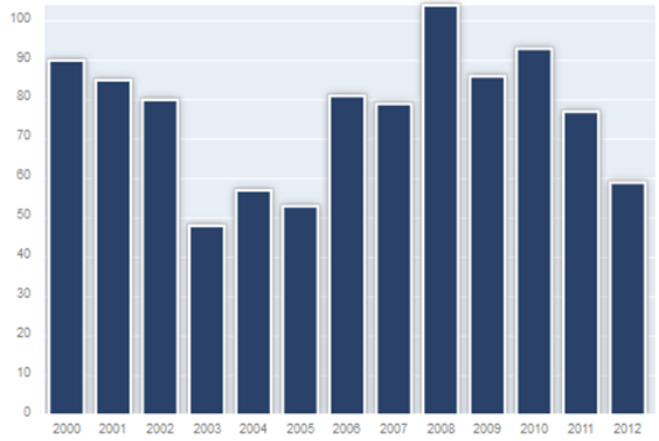


	Country	Complainants
1	United States	9718
2	France	2728
3	United Kingdom	1970
4	Germany	1469
5	Switzerland	1332
6	Spain	992
7	Italy	919
8	Denmark	768
9	Netherlands	643
10	Sweden	461

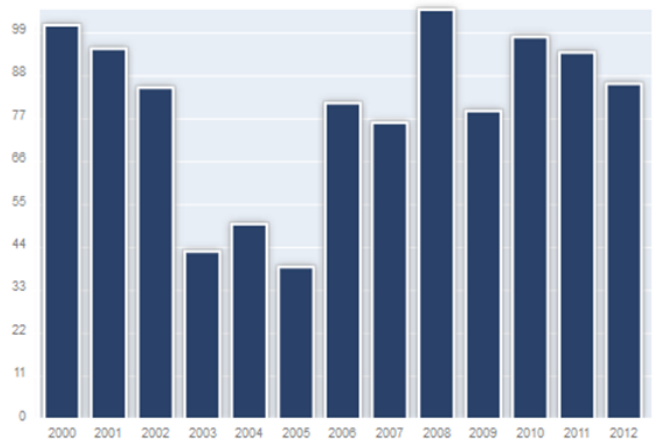
	Country	Respondents
1	United States	8785
2	China	2061
3	United Kingdom	1970
4	Spain	1032
5	Canada	969
6	Australia	792
7	Republic of Korea	779
8	France	774
9	Netherlands	609
10	India	447

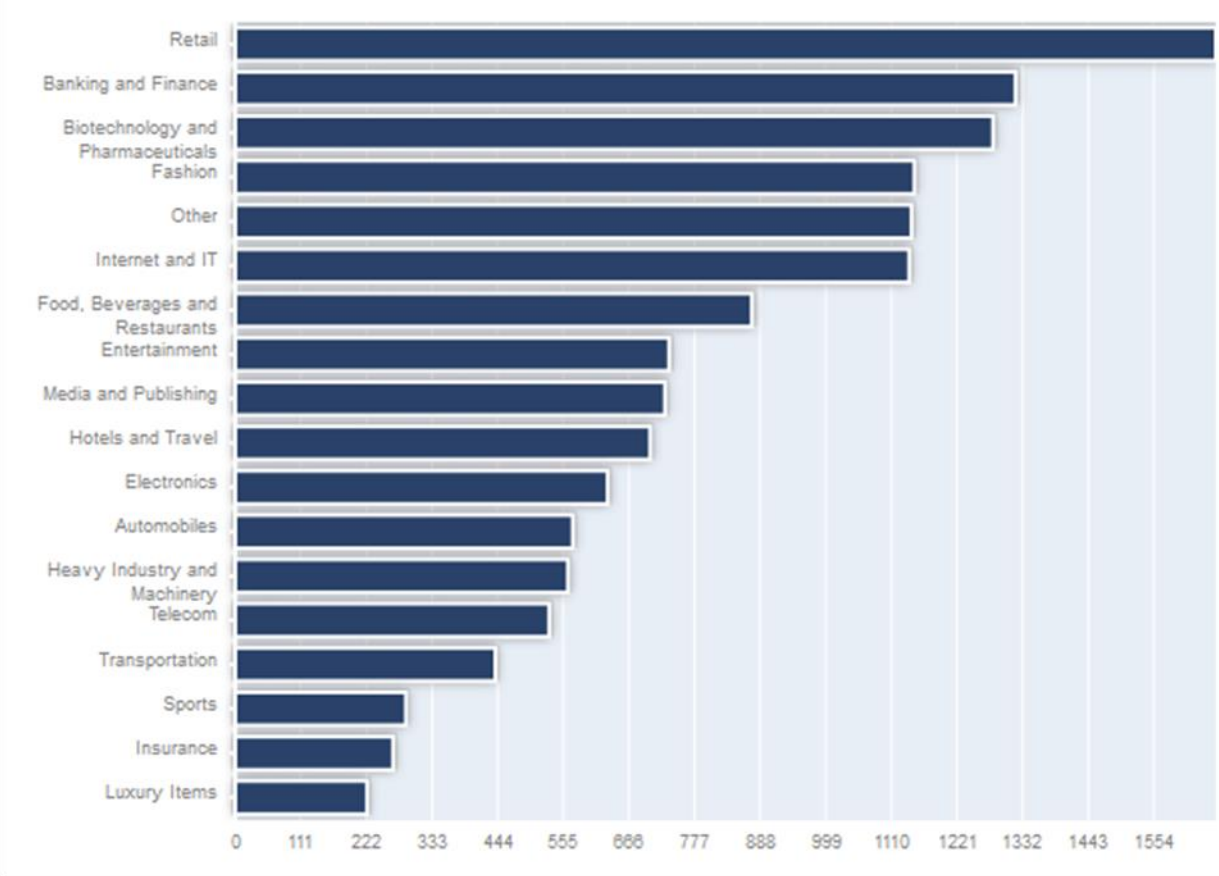
Número de casos en España

Demandantes



Demandados





Fuente: WIPO (World Intellectual Property Organization)
http://www.wipo.int/amc/en/domains/statistics/

DNS: Asociación de Nombres de Dominio con Direcciones

- Para asociar nombres de dominio a direcciones IP se utilizan **servidores de nombres**
- Se utiliza este nombre tanto para los programas como para los computadores donde se ejecutan
- Los servidores de nombre se organizan, *conceptualmente*, según una estructura de árbol
- Físicamente, los servidores están en localizaciones arbitrarias
- Cuando les llega un nombre a resolver lo envían al servidor adecuado del siguiente nivel
- Cada servidor conoce los servidores de nivel superior

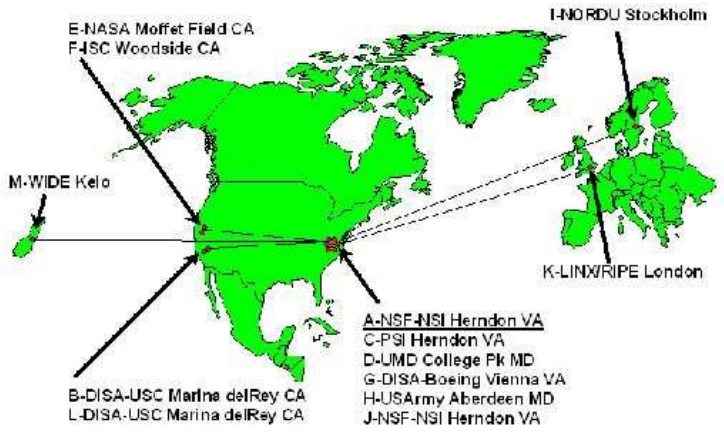
DNS: Tipos de Servidores

- **Primarios (*Primary Name Servers*):** Almacenan la información de su zona en una base de datos local. Son responsables de mantener la información actualizada y cualquier cambio debe ser notificado a este servidor
- **Secundarios (*Secundary Name Servers*):** Son aquellos que obtienen los datos de su zona desde otro servidor que tenga autoridad para esa zona. El proceso de copia de la información se denomina *transferencia de zona.*
- **Maestros (*Master Name Servers*):** son los que transfieren las zonas a los servidores secundarios. Cuando un servidor secundario arranca busca un servidor maestro y realiza la transferencia de zona (puede ser a la vez un servidor primario o secundario de esa zona)
- **Locales (*Caching-only servers*):** no tienen autoridad sobre ningún dominio: se limitan a contactar con otros servidores para resolver las peticiones de los clientes DNS. Estos servidores mantienen una *memoria caché* con las últimas preguntas contestadas. Si encuentra la dirección IP solicitada, se la devuelve al cliente; si no, consulta a otros servidores, apunta la respuesta y responde al cliente.

DNS: Servidores Raíz

- Las direcciones IP de los dominios superiores no se incluyen en el DNS porque no son parte del propio dominio.
- Para consultar hosts externos se consulta a los servidores raíz, cuyas direcciones IP están presentes en un fichero de configuración del sistema y se cargan en el caché del DNS al iniciar el servidor.
- Los servidores raíz proporcionan referencias directas a servidores de los dominios de segundo nivel, como COM, EDU, GOV, etc.

A	Network Solutions, Herndon, Virginia, USA
B	Instit. Ciencias Info, Univ del Sur de California, USA
C	PSINet, Virginia, USA
D	Universidad de Maryland, USA
E	NASA, en Mountain View, California, USA
F	Internet Softw. Consort, Palo Alto, California, USA
G	Ag. de Sist. de Info. de Defensa, California, USA
H	Lab. de Invest. del Ejercito, Maryland, USA
I	NORDUnet, Estocolmo, Suecia
J	(TBD), Virginia, USA
K	RIPE-NCC, Londres, Inglaterra
L	(TBD), California, USA
M	Wide Project, Universidad de Tokyo, Japón




Canada
United States
Россия
China
Australia
DNS ROOT SERVER LOCATIONS

DNS: Funciones del Cliente

- Interrogar al servidor DNS: Tres métodos de búsqueda:
  - Recursiva: obliga al servidor DNS a que responda aunque tenga que consultar a otros servidores
  - Iterativa: el servidor contesta si tiene la información y si no, le remite la dirección de otro servidor capaz de resolver
  - Inversa: permite dada una IP, consultar el nombre. Para ello se ha creado un dominio especial llamado "*in-addr.arpa*"
- Interpretar las respuestas que pueden ser registros de recursos (RR) o errores
- Devolver la información al programa que realiza la petición al cliente DNS

DNS: Resolución de Nombres

- El cliente elabora una consulta de nombre de dominio que incluye :el
  - nombre a resolver,
  - la clase del nombre (dirección de máquina, dirección de servidor de correo,...)
- Envía la consulta a su servidor de nombres local (debe conocer su dirección IP)
- La consulta se puede hacer por UDP o TCP
  - Es más habitual hacerla por UDP (menos sobrecarga)
- Cuando el servidor de nombres local recibe la petición:
  - Si el nombre pertenece a su dominio, traduce el nombre (a su dirección IP) y envía la respuesta al cliente
- Si no puede resolver el nombre:
  - El servidor contacta con el servidor de nombres raíz (realizando ahora el papel de cliente) que pueda resolver la consulta
  - Si este último no puede resolver la consulta, contacta con otro, y así sucesivamente

DNS: Búsqueda (Consulta) Recurrente

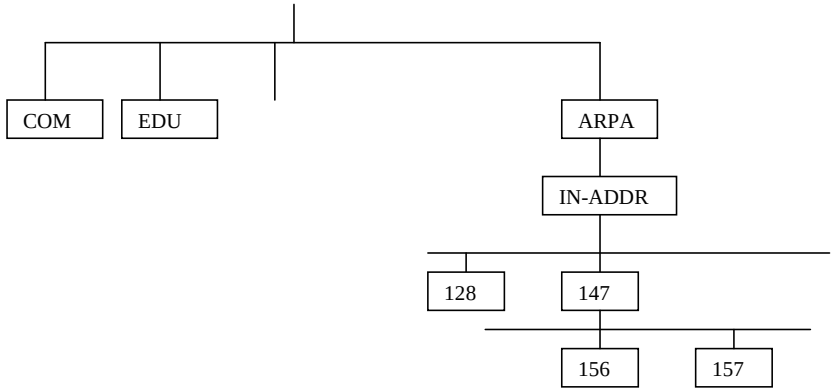
- Estamos en un ordenador (cliente DNS) fuera de la Universidad y formula una *pregunta recursiva* ¿IP de www.unican.es? a nuestro servidor DNS local (generalmente el proveedor de Internet ISP):
- 1. El servidor local es el responsable de resolver la pregunta, aunque para ello tenga que reenviar la pregunta a otros servidores. Si se ha solicitado información local, el servidor extrae la respuesta de su propia base de datos. Si es sobre un ordenador externo al ISP, el servidor comprueba su caché. Si no tiene la dirección IP entonces formulará una *pregunta iterativa* al servidor del dominio raíz.
- 2. El servidor del dominio raíz no conoce la dirección IP solicitada, pero devuelve la dirección del servidor del dominio *es*.
- 3. El servidor local reenvía la pregunta iterativa al servidor del dominio *es*. que tampoco conoce la dirección IP preguntada, aunque sí conoce la dirección del servidor del dominio *unican.es,* por lo que devuelve esta dirección.
- 4. El servidor local vuelve a reenviar la pregunta iterativa al servidor del dominio *unican.es*. Que ahora si conoce la dirección IP de www.unican.es y devuelve esta dirección al servidor local.
- 5. El servidor local se la reenvía a nuestro ordenador, al mismo tiempo que la almacena en la propia caché.

.

- EL TIEMPO DE VALIDEZ DE LA RESPUESTA EN LA CACHE SE CONFIGURA EN LOS SERVIDORES REMOTOS DE CONFIANZA Y SE ENVIA COMO PARTE DE LA RESPUESTA.

DNS: Búsqueda Inversa

- Para evitar una búsqueda exhaustiva por todo el espacio de nombres de dominio, se utiliza un dominio especial llamado *in-addr.arpa*.
- Cuando un cliente DNS desea conocer el nombre de dominio asociado a la dirección IP *w.x.y.z* realiza una pregunta inversa a ***z.y.x.w.in-addr.arpa***.
- La inversión de los bytes es necesaria debido a que los nombres de dominio son más genéricos por la derecha, al contrario que ocurre con las direcciones IP.
- La organización que posee una dirección de red es responsable de registrar todas sus traducciones de dirección a nombre en la base de datos del DNS.
- Esto se hace en una tabla que es independiente de las correspondencias entre nombre y direcciones.
- El dominio ***in-addr.arpa*** se creó para apuntar hacia todas esas tablas de red
- **Destacar que muchos servidores FTP, WWW, NEWS,... No aceptarán conexiones de máquinas de las cuales no son capaces de resolver el nombre, por eso el mapeo inverso es obligado.**



DNS: Formato de los mensajes

- El cliente envía su solicitud (pregunta) en un mensaje formateado y el servidor añade la información requerida en dichos campos. Este formato permite realizar varias consultas.

0 bit…..16 bit ……..32 bit

IDENTIFICACIÓN de la pregunta	PARÁMETROS
Nº DE SOLICITUDES	Nº DE RESPUESTAS (1)
Nº DE REG. AUTORIDAD (1)	Nº DE REGISTROS ADICIONALES (1)
Consulta/s (sección de solicitudes)	
RR de respuestas (sección de respuestas)	
RR de autoridad (sección de respuestas)	
RR de información adicional (sección de respuestas)	

(1)rellenado por DNS

Tipos de Registros

A (Address). Es el registro más usado, que define una dirección IP y el nombre asignado al host. Generalmente existen varios en un dominio.

PTR (**Pointer – (Indicador**) También conocido como 'registro inverso', funciona a la inversa del registro A, traduciendo IPs en nombres de dominio.

MX (Mail eXchanger). Se usa para identificar servidores de correo, se pueden definir dos o más servidores de correo para un dominio, siendo que el orden implica su prioridad. Debe haber al menos uno para un dominio.

CNAME (Canonical Name). Es un alias que se asigna a un host que tiene una dirección IP valida y que responde a diversos nombres. Pueden declararse varios para un host.

NS (Name Server). Define los servidores de nombre principales de un dominio. Debe haber al menos uno y pueden declararse varios para un dominio.

SOA (Start Of Authority). Este es el primer registro de la zona y sólo puede haber uno en cada archivo de la zona y sólo está presente si el servidor es autoritario del dominio. Especifica el servidor DNS primario del dominio, la cuenta de correo del administrador y tiempo de refresco de los servidores secundarios.

LOC (localización) Permite indicar las coordenadas del dominio.

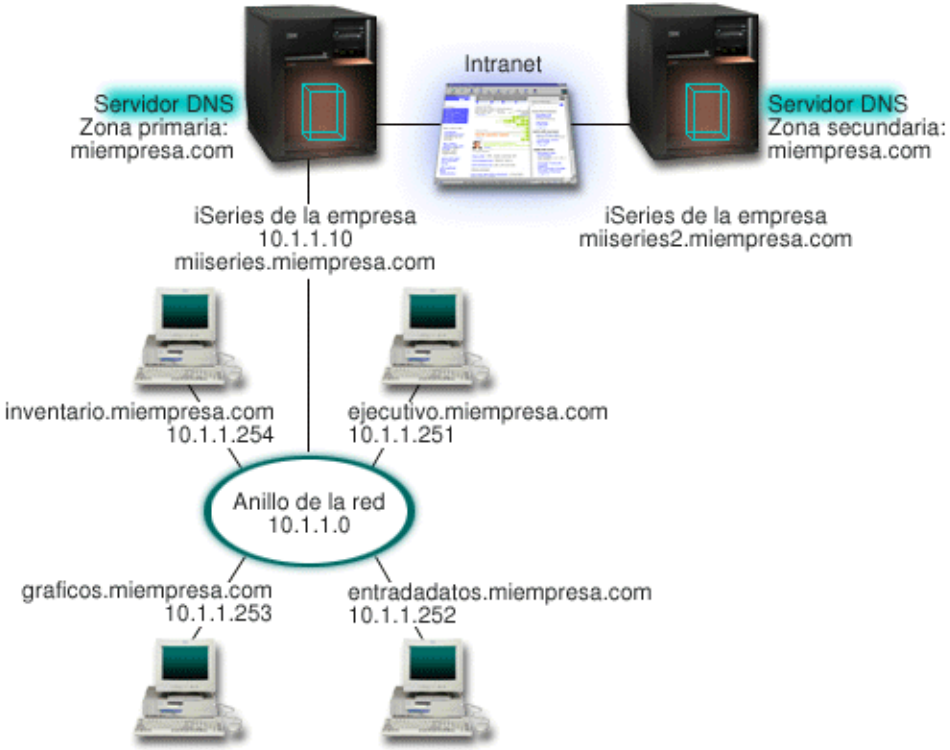
TXT (Text): Permite asociar información adicional a un dominio. Esto se utiliza para otros fines, como el almacenamiento de claves de cifrado.

HINFO: Éste registro especifica los recursos de información del host, es decir, especifica la CPU de la máquina y el S.O (sistema operativo).

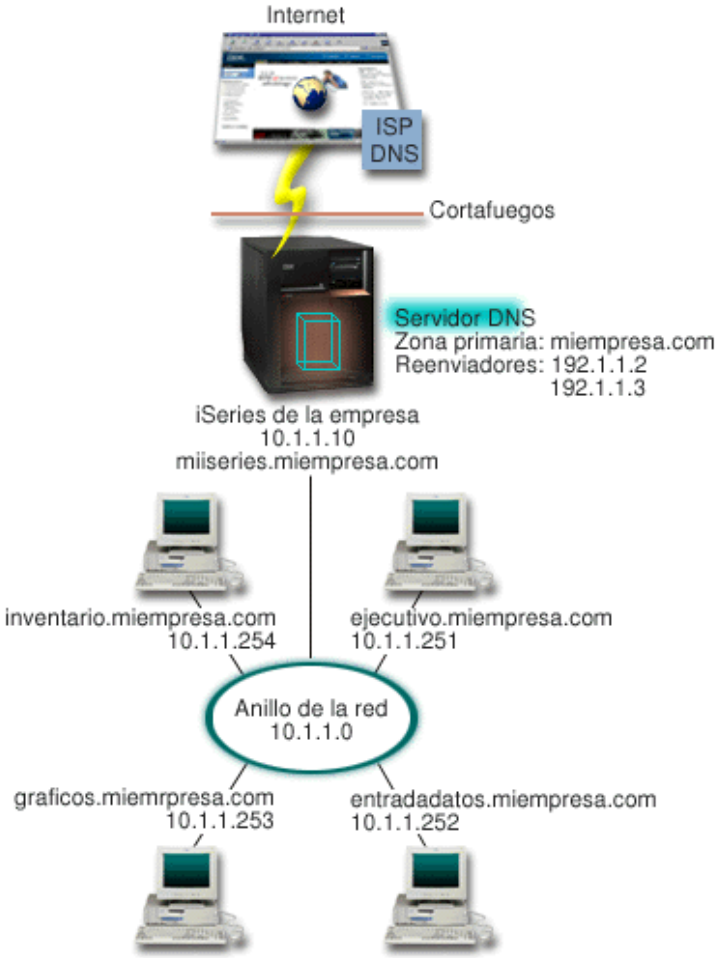
Name	Type	Value	Select
admin	A	216.194.67.119	☐
localhost.site-helper.com.	A	127.0.0.1	☐
reseller	A	216.194.67.119	☐
site-helper.com.	A	216.194.67.119	☐
site-helper.com.	NS	ns1.jbmc-software.com.	☐
site-helper.com.	NS	ns2.jbmc-software.com.	☐
site-helper.com.	MX	0	☐
ftp	CNAME	site-helper.com.	☐
mail	CNAME	site-helper.com.	☐
www	CNAME	site-helper.com.	☐

```
@       IN      SOA     site-helper.com. root.lsite-helper.com. (
                        199609206       ; Numero de Serie, fecha de hoy + numero de serie de hoy
                        10800           ; Tasa de Refresco, en segundos
                        7200            ; Tasa de Reintento, en segundos
                        10800           ; Caducidad para secundario, en segundos
                        86400 )         ; Validez para Clientes, en segundos
                NS      lns1.jbmc-software.com.
                NS      ns2.jbmc-software.com.
                MX      0  ; Intercambiador Primario de Correo

admin       A       216.194.67.119
localhost .site-helper.com      A       127.0.0.1
%router         A       216.194.67.1
reseller    A       216.194.67.119
site-helper.com     A       216.194.67.119

ns              CNAME site-helper.com.
ftp             CNAME site-helper.com.
www             CNAME site-helper.com.
mail            CNAME site-helper.com.
news            CNAME site-helper.com.
```

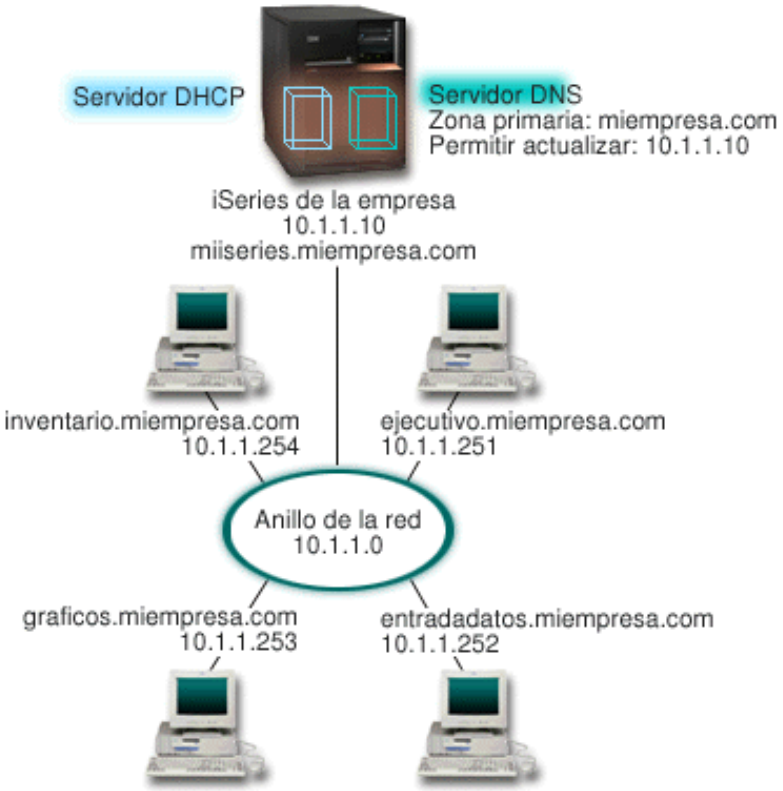
DNS Intranet



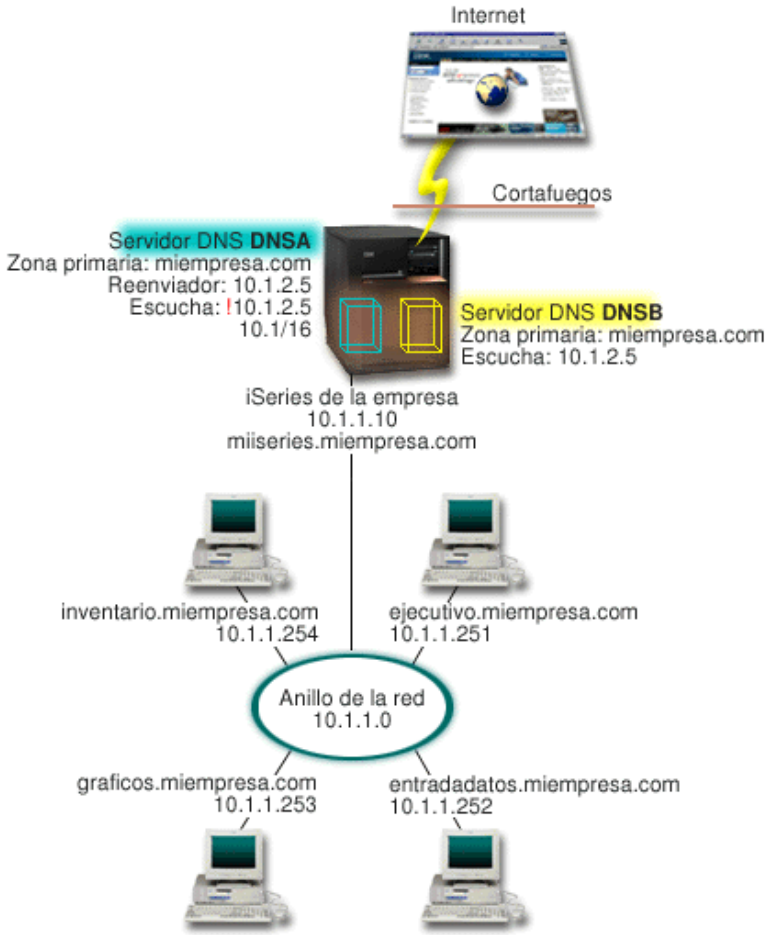
DNS con acceso a Internet



DNS + DHCP



DNS Partido



- *Clientes:*
  - *Comando Nslookup* (*Win2K y UNIX*).
  - *Comando Hosts* y fichero */etc/resolv.conf*(*UNIX*).
- *Servidores:*
  - *"named", dentro del paquete "bind"*

El servicio de servidores públicos DNS de Google

Desde Diciembre del 2009 en que comenzó a funcionar el servicio de los servidores públicos DNS de Google, han contribuido a que la internet sea más rápida. Google presta dicho servicio de forma gratuita

Google 8.8.8.8 8.8.4.4

Para el protocolo IPv4 (actual)
➔ *Servidor primario: 8.8.8.8*
➔ *Servidor secundario: 8.8.4.4*
Para el protocolo IPv6 (nuevo protocolo de internet)
➔ *Servidor primario: 2001:4860:4860::8888*
➔ *Servidor secundario: 2001:4860:4860::8844*

OpenDNS

Dirección IP de los servidores de OpenDNS
➔ *Servidor primario: 208.67.222.222*
➔ *Servidor secundario: 208.67.220.220*

Servicios de Noticias (NEWS)

- News o Usenet News (User's Network) – RFC850
- Sistema mundial distribuido de mensajes (artículos)
- Accesible a través de Internet u otros servicios de red
- Conjunto de foros (grupos de news, newsgroups) clasificados jerárquicamente por tema (todos :-)
- + de 30.000 grupos (moderados o no), M mensajes/diarios

- NO es:
  - Organización, servicio público, red independiente, ...
- SI es:
  - Conjunto de personas intercambiando información

NEWS: Servicio

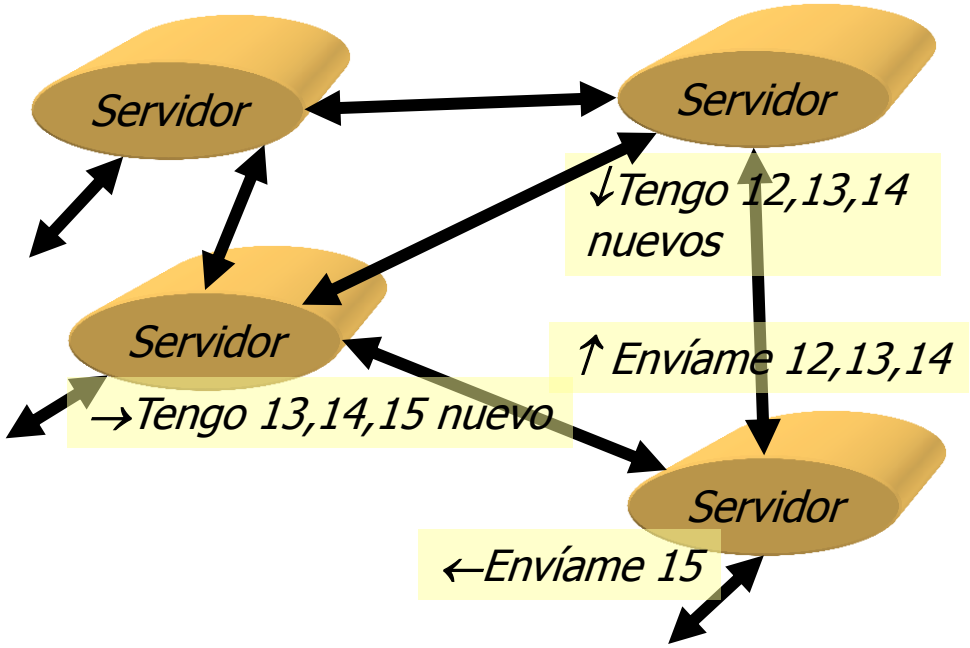
- Servidores
  - Por todo el mundo
  - Conjunto de grupos soportados en cada servidor
  - Intercambio de mensajes con vecinos interesados
    - Propagación en pocos minutos
    - Cada grupo parece el mismo en cualquier parte del mundo
  - Diseño distribuido robusto
- Clientes
  - Lectores de news (NNTP)
  - Recepción / envío de mensajes

NEWS: Jerarquía de grupos

- Jerarquía
  - Categorías principales
    - alt - alternative, popular topics
    - comp - computer science subjects
    - humanities - humanities subjects
    - misc - miscellaneous groups
    - news - news topics
    - rec - recreational subjects
    - sci - science topics
    - soc - sociological subjects
    - talk - controversial topics
  - Otras jerarquías de primer nivel (casi 1.000)

NEWS: Funcionamiento

- Cada servidor se comunica con:
  - Sus usuarios locales
  - Otros servidores de su vecindad
- Un servidor ofrece (pushing) a sus vecinos mensajes.
- Aceptan (pulling) los que no han recibido por otro camino



NNTP: Network News Transfer Protocol

- RFC977
- Protocolo para distribución, petición, obtención y envío de artículos de news
- Modelo cliente-servidor
- Válido para sistemas no Usenet
- NNTP especifica:
  - Comunicación entre servidores y cliente-servidor
- Distribución por inundación controlada entre servidores conectados

NNTP: Funcionamiento

- Servidor news
  - Acepta conexiones de clientes y otros servidores
  - TCP/119 ------ SSL 563
  - Interfaz con BD News
- Comandos
- Respuestas
  - Textuales
  - Estado
    - 1xx: Informativo
    - 2xx: Ok
    - 3xx: Ok, enviar más
    - 4xx: Comando correcto pero no ejecutado
    - 5xx: Comando incorrecto

NNTP: Comandos

Comando	Significado
ARTICLE <id-mens>|<nnnn>	recibir texto mensaje
HEAD <id-mens>|<nnnn>	recibir cabecera
BODY <id-mens>|<nnnn>	recibir cuerpo
STAT <id-mens>|<nnnn>	ver qué artículo apunta el cursor
GROUP ggg	selección grupo, devuelve nºestimado, nº 1º y último
HELP	comandos soportados
IHAVE <id-mens>	informa al servidor que tiene el mensaje
LAST	mover el cursor al último mensaje
LIST	devuelve lista de grupos y su info
NEWGROUPS fecha hora [GMT][dist]	grupos creados desde ...
NEWNEWS grupo fecha hora [GMT]	lista de mensajes desde ...
NEXT	cursor al siguiente mensaje
POST	enviar (publicar) un mensaje (formato RFC850)
QUIT	cierre conexión
SLAVE	informa que el cliente es otro servidor
XOVER	vista general de artículos para su presentación

NNTP: Ejemplo de consulta

C: STAT 10110 (client selects an article to read)
S: 223 10110 <23445@sdcsvax.ARPA> article retrieved - statistics only (article 10110 selected, its message-id is <23445@sdcsvax.ARPA>)
C: HEAD (client examines the header)
S: 221 10110 <23445@sdcsvax.ARPA> article retrieved - head follows (text of the header appears here)
S: .
C: BODY (client wants to see the text body of the article)
S: 222 10110 <23445@sdcsvax.ARPA> article retrieved - body follows (body text here)
S: .
C: NEXT (client selects next article in group)
S: 223 10113 <21495@nudebch.uucp> article retrieved - statistics only (article 10113 was next in group)
C: QUIT (client finishes session)
S: 205 goodbye.

NNTP: Ejemplo de consulta (y II)

C: STAT 10110 (client selects an article to read)
S: 223 10110 <23445@sdcsvax.ARPA> article retrieved - statistics only (article 10110 selected, its message-id is <23445@sdcsvax.ARPA>)
C: HEAD (client examines the header)
S: 221 10110 <23445@sdcsvax.ARPA> article retrieved - head follows (text of the header appears here)
S: .
C: BODY (client wants to see the text body of the article)
S: 222 10110 <23445@sdcsvax.ARPA> article retrieved - body follows (body text here)
S: .
C: NEXT (client selects next article in group)
S: 223 10113 <21495@nudebch.uucp> article retrieved - statistics only (article 10113 was next in group)
C: QUIT (client finishes session)
S: 205 goodbye.

NNTP: Ejemplo de transferencia

S: (listens at TCP port 119)
C: (requests connection on TCP port 119)
S: 201 Foobar NNTP server ready (no posting)
(asks for new newsgroups since 2 am, May 15, 1985)
C: NEWGROUPS 850515 020000
S: 235 New newsgroups since 850515 follow
S: net.fluff
S: net.lint
S: .
(client asks for new news articles since 2 am, May 15, 1985)
C: NEWNEWS * 850515 020000
S: 230 New news since 850515 020000 follows
S: <87623@baz.UUCP>
S: <17872@GOLD.CSNET>
S: .

NNTP: Ejemplo de transferencia (pulling)

(client asks for article <1772@foo.UUCP>)
C: ARTICLE <1772@foo.UUCP>
S: 220 <1772@foo.UUCP> All of article follows
S: (sends entire message)
S: .
(client asks for article <87623@baz.UUCP>)
C: ARTICLE <87623@baz.UUCP>
S: 220 <87623@baz.UUCP> All of article follows
S: (sends entire message)
S: .
(client asks for article <17872@GOLD.CSNET>
C: ARTICLE <17872@GOLD.CSNET>
S: 220 <17872@GOLD.CSNET> All of article follows
S: (sends entire message)
S: .

NNTP: Ejemplo de transferencia (pushing)

(client offers an article it has received recently)

C: IHAVE <4105@ucbvax.ARPA>

S: 435 Already seen that one, where you been?

(client offers another article)

C: IHAVE <4106@ucbvax.ARPA>

S: 335 News to me! to end.

C: (sends article)

C: .

S: 235 Article transferred successfully. Thanks.

(or)

S: 436 Transfer failed.

(client is all through with the session)

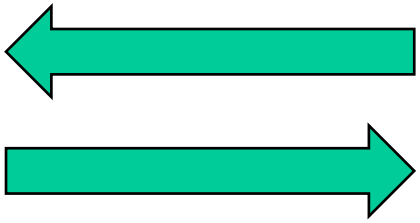
C: QUIT

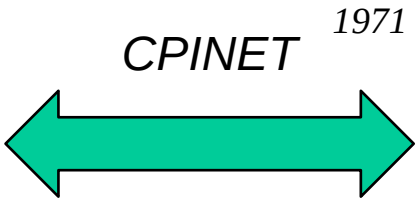
S: 205 Foobar NNTP server bids you farewell.

Mensajería y Correo electrónico

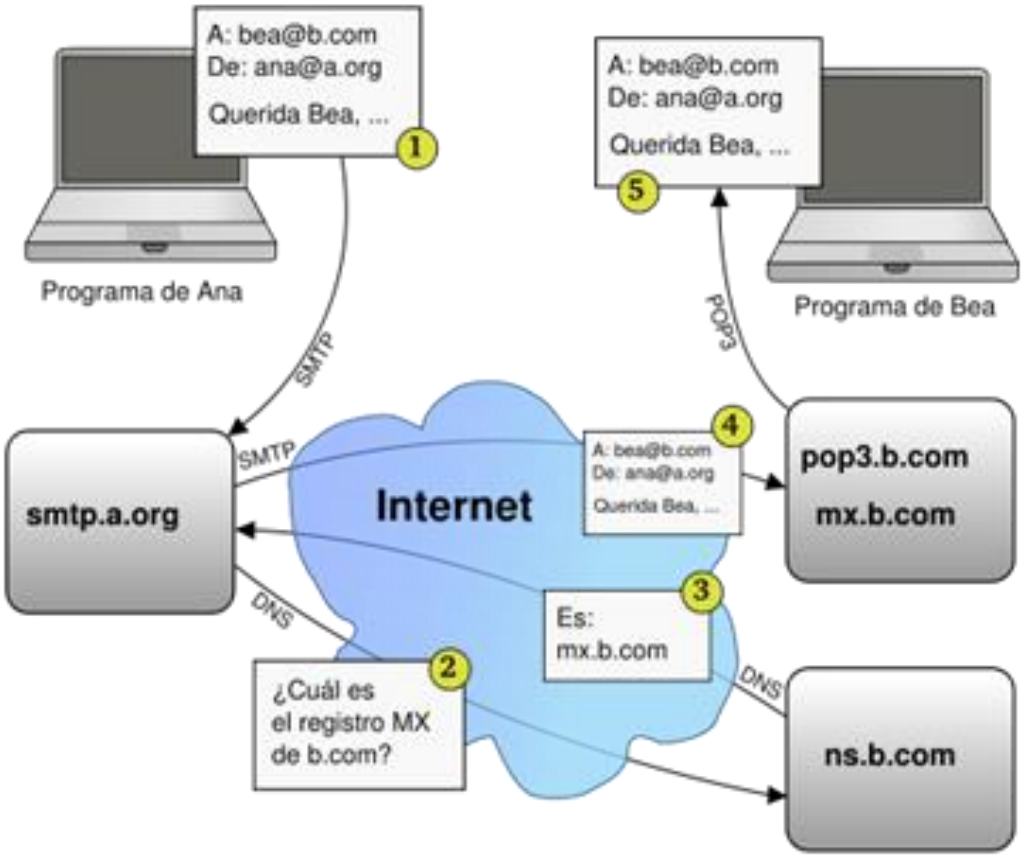
Tomlinson, a finales de los 60 desarrolla el primer sistema de mensajería entre los usuarios de un ordenador

"Fui el primero en llegar, así que pude elegir a mis anchas…."

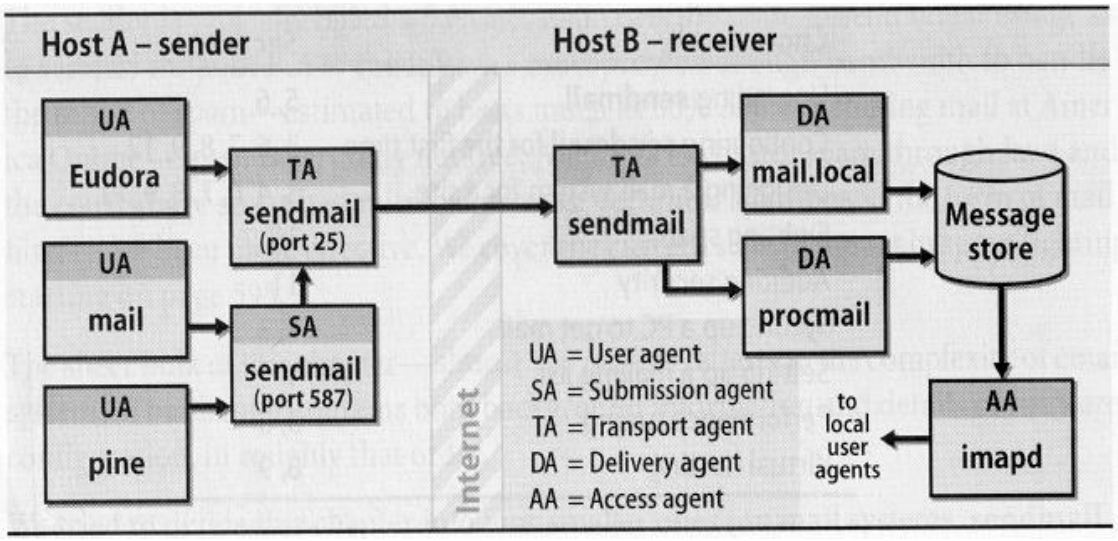




El correo electrónico, tal y como lo conocemos



Componentes del sistema de correo



- ***Agente de usuario (MUA ≡ Mail User Agent)***
  - *Leer, escribir correo*
- ***Agente de transporte (MTA ≡ Mail Transport Agent)***
  - *Encaminamiento mensajes*
- ***Agente de reparto (MDA ≡ Mail Delivery Agent)***
  - *Entrega mensajes al almacén*
- ***Almacén de mensajes***
- ***Agente acceso***
  - *Conecta MUA con el almacén de mensajes*
  - *POP, IMAP*
- ***Agente "submission" de correo***
  - *Parte del trabajo del MTA*

Componentes del sistema de correo

MUA

- *– Lectura y escritura de mensajes*
- *– Entregan mensajes a MTAs*
- *– Reciben mensajes de agentes de acceso*
- *– Inicialmente sólo texto*
- *– MIME: codificación*
  - *Formatos de textos*
  - *Anexos (virus)*

– Ejemplos: /bin/mail, Mail, mailx, mush, elm, mutt, mh, pine, emacs, Zmail, Eudora, Netscape Messenger, Outlook Express

– Varios MUAs en una misma máquina

MTA

- *– Aceptan correo de MUAs y de otros MTAs*
- *– Interpretan las direcciones de destino*
- *– Obtienen los mensajes para su entrega a las máquinas adecuadas*
- *– La mayoría también hace de SA*

– SMTP=Simple Mail Transfer Protocol (RFC821)

– ESMTP=Extended SMTP (RFCs 1869, 1870, 1891, 1985)

– Ejemplos: sendmail, Postfix, smail, zmailer, upas*

*– **Puerto 25***

MDA

- *– Aceptan correo de MTAs*
- *– Entrega al destinatario apropiado*
- *– Agentes de reparto diferentes según el tipo de destinatario*

-Usuarios locales: /bin/mail

- Usuarios remotos: popd, popper, imapd

- Programas, ficheros: /bin/sh

- Listas de correo: ??

MSA

- *–MTAs sobrecargados - Preprocesado mensajes*
- *– RFC2476: MSAs: comprobación errores: Nombres de dominios correctos y Cabeceras*

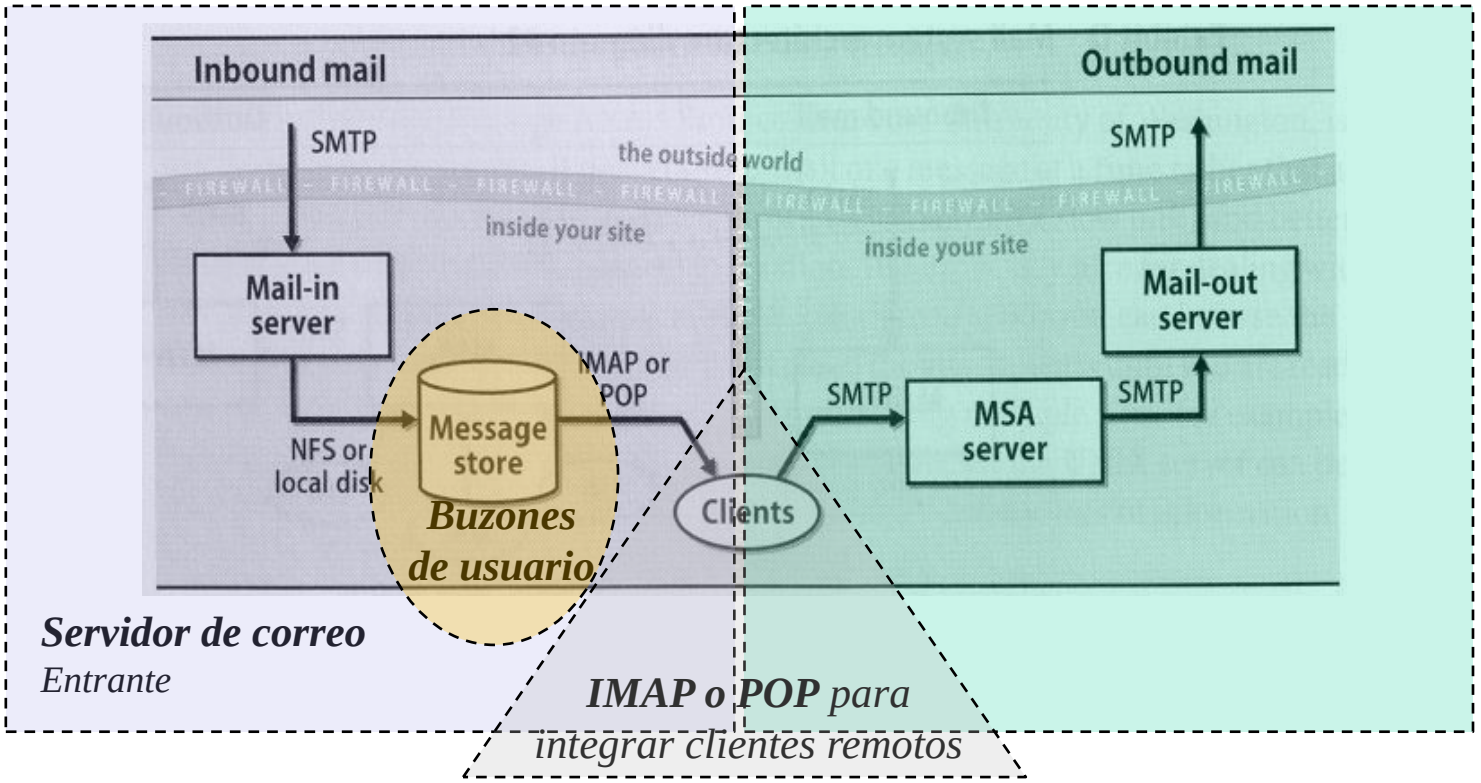
– sendmail:MSA y MTA (servicios en distintos puertos)

*– **Puerto 587***

Correo Electrónico: Arquitectura

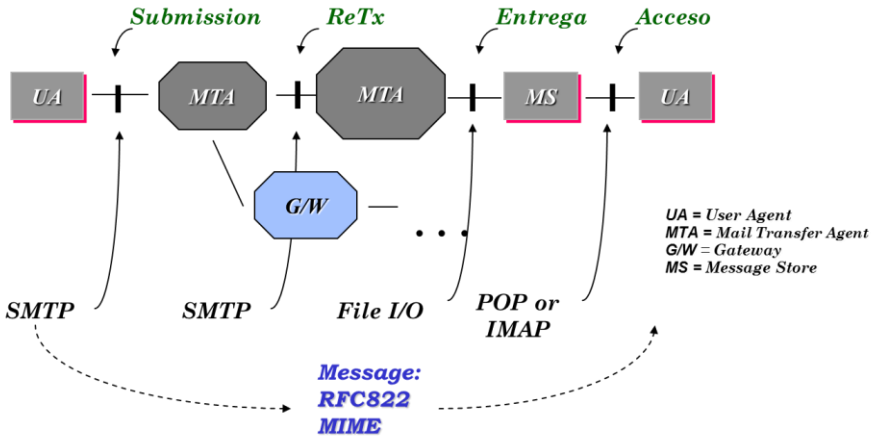
Registros MX

(Mail eXchange, DNS)



Correo Electrónico: Protocolos

Función	Protocolos
Composición de mensajes:	RFC 822 y MIME
Envío:	SMTP y ESMTP
Localización:	MX
Reenvío:	SMTP
Recepción remota:	IMAP4: Consulta y manipulación remota POP3: Transferencia
Encaminamiento (RFC 974)	Dependendiente del host destino Por defecto, se envía el mensaje directamente al host de destino: el encaminamiento lo hace la capa IP de forma transparente La mayoría de las máquinas dirigen su correo entrante a un servidor de correo, para hacer luego la distribución local Registros MX (*Mail Exchanger*) del dominio local en la base de datos DNS (*named.hosts*) Prioridad del *exchanger* (o coste) El MTA envía el mensaje al MX de menor coste Si ese falla, lo intentará con otro de mayor coste Nunca enviará a un MX con coste igual o mayor que el suyo: evitar ciclos de envío



Correo electrónico: Direcciones

- Dirección absoluta
  - Estándar de Internet - RFC 822: `uc2521x@alumnos.unican.es`
  - DECnet: `user::machine@passerelle.dans.internet`
  - X.400: conjunto de pares atributo-valor
  - Fidonet: código numérico `zona:red/nodo.punto`
- Dirección con ruta
  - UUCP (Notación *bang path)*: `trayecto!host!usuario`
  - Híbrida: `hostA!usuario@hostB` (el símbolo '@' tiene prioridad sobre '!')
  - Explícita: `<@ibp.fr,@uvsq.fr:jean@jussieu.fr>` NO
  - RFC 1123: `jean % jussieu.fr % uvsq.fr @ ibp.fr` SI
  - Extensión dir. locales: `jean+toto@jussieu.fr`

Correo electrónico: Mensajes

- Sobre
  - Dónde se entrega el mensaje o a quién se devuelve
  - Para evitar bucles (destinatarios múltiples)
- Cabeceras
  - Lista de campos Propiedad/Valor (RFC822)
    - Fecha, agentes de transporte atravesados, ...
    - Campos obligatorios, opcionales y extensiones
- Cuerpo del mensaje
  - Contenido
    - Texto
    - Codificación de contenido binario (MIME)

```
Received: from alumnoscorreo.unican.es ([155.210.152.58])
          by alumnoscorreo.unican.es (8.9.1/8.9.1) with ESMTP id MAA31230
          for <uc2521x@alumnoscorreo.unican.es>; Wed, 21 Feb 2001 12:58:45 +0100 (MET)
Message-ID: <3A93ADE0.10E568F7@alumnoscorreo.unican.es>
Date: Wed, 21 Feb 2001 13:00:40 +0100
From: Pepito Grillo <uc666@alumnoscorreo.unican.es>
To: uc2521x <uc2521x@alumnoscorreo.unican.es>
Subject: Quedada
Status: RO

El viernes a las 9, de marcha.
```

Correo electrónico: Cabeceras

- Especificación **RFC 822:**
  - Formato: `<Campo>:<Contenido><CRLF>`
  - Múltiples líneas: las siguientes a la primera empiezan por una tabulación o un espacio en blanco
  - Se pueden incluir comentarios entre parentesis en el contenido de la cabecera `(Comentario)`
  - Generalmente, el MUA añade las cabeceras necesarias
  - Las cabeceras contienen el sobre: no se pueden cifrar
  - Cabeceras más comunes
    - `Received:` cada MTA atravesado por el mensaje añade una línea con información del encaminamiento seguido.
    - `From: , Sender:, Reply-To:` dirección de correo del remitente (y posiblemente su nombre real)
    - `To: , Cc:, Bcc:` dirección destino
    - `Date:` fecha y hora de envío
    - `Message-ID:` identificador único de mensaje
    - `Subject:` tema del mensaje (opcional)
    - `X-*:` Campos no estándar definidos por usuarios

Correo electrónico: Cuerpo

- RFC 822 sólo permite texto codificado como US-ASCII de 7 bits:
  - Ficheros binarios ¿?
  - Texto con otra codificación ¿?
- Método tradicional UNIX: uuencode/uudecode
- Macintosh: BinHex
- MIME ≡ *Multipurpose Internet Mail Extensions*
  - Extensiones Multimedia para Correo Internet (y +)
  - Especificación para adaptar el transporte de objetos multimedia compuestos a la infraestructura existente
  - Formato interno invisible a los usuarios
  - Encapsulamiento y transporte de objetos en Internet
  - RFCs 2045-2049

MIME: Multipurpose Internet Mail Extensions

- Amplía la capacidad de representación de los mensajes
  - Múltiples cuerpos dentro del contenido
  - Contenido de cualquier tipo, no sólo texto
  - Juego de caracteres diferente del US-ASCII
- Nuevos campos de cabecera
  - `MIME-Version:` 1.0
  - `Content-Type:` tipo y subtipo de contenido
  - `Content-Transfer-Encoding:` codificación usada y dominio del resultado
  - `Content-ID:` permite que un cuerpo haga referencia a otro, especialmente con tipos compuestos (identificador único)
  - `Content-Description:` información descriptiva asociada a un cuerpo (opcional)

Codificación

- MIME utiliza diferentes mecanismos para convertir datos al formato de 7 bits del US-ASCII en lo que se conoce como **"transfer-encoding"**
  - Quoted-printable
  - Base 64
  - Binary (sólo ESMTP)
  - 7bit
  - 8bit (sólo ESMTP)
  - X-Token

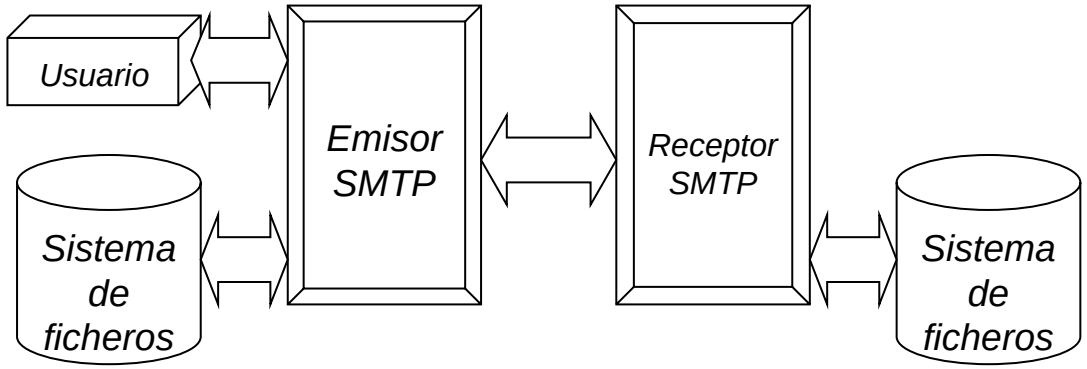
- Codificación quoted-printable
  - Mayoría texto: no se codifica (7 bits, caracteres del juego US-ASCII)
  - Caracteres especiales: se transforman
    - '=' + codif. ASCII en Hexa
    - ª ->=A6, =->=D3
  - Resultado casi legible sin decodificar
  - Ejemplo
    - Texto: *El camión se salió de la cañada*
    - Codificación: `El cami=F3n se sali=F3 de la ca=F1ada`
  - <http://www.freesoft.org/CIE/RFC/1521/6.htm>

- Codificación base 64
  - RFC 152 <http://www.ietf.org/rfc/rfc1521.txt>
  - Similar / evolución uuencode
  - Emplea un subconjunto del US-ASCII de 64 caracteres
  - Grupos de 24 bits de entrada → 4 grupos de 6 bits → 4 caracteres codificados del *alfabeto base 64* → 4 ASCII → 32 bits
    - Incrementa el tamaño de los mensajes un 33%
  - Grupo de menos de 24 bits: se rellena con bits 0
  - Decodificación:
    - Relleno con '=' para que el nº de caracteres a la salida sea múltiplo de 4
    - Se ignoran caracteres que no estén en la tabla (CR, LF, *, ...)
  - http://www.freesoft.org/CIE/RFC/1521/7.htm

Valor	Código	Valor	Código	Valor	Código	Valor	Código	Valor	Código
0	A	13	N	26	a	39	n	52	0
1	B	14	O	27	b	40	o	53	1
2	C	15	P	28	c	41	p	54	2
3	D	16	Q	29	d	42	q	55	3
4	E	17	R	30	e	43	r	56	4
5	F	18	S	31	f	44	s	57	5
6	G	19	T	32	g	45	t	58	6
7	H	20	U	33	h	46	u	59	7
8	I	21	V	34	i	47	v	60	8
9	J	22	W	35	j	48	w	61	9
10	K	23	X	36	k	49	x	62	+
11	L	24	Y	37	l	50	y	63	/
12	M	25	Z	38	m	51	z	(pad)	=

Correo electrónico: SMTP

- SMTP ≡ Simple Mail Transfer Protocol
  - Protocolo Simple para Transferencia de Correo
- Objetivo: envío de correo de manera fiable y eficiente
- Independiente del sistema de transmisión
  - Requiere canal de datos fiable y ordenado
- Especificación: RFC 821
- Modelo:
  - Comando del cliente ↔ respuesta del servidor (código de retorno)
- Puerto TCP/25



SMTP: Funcionamiento

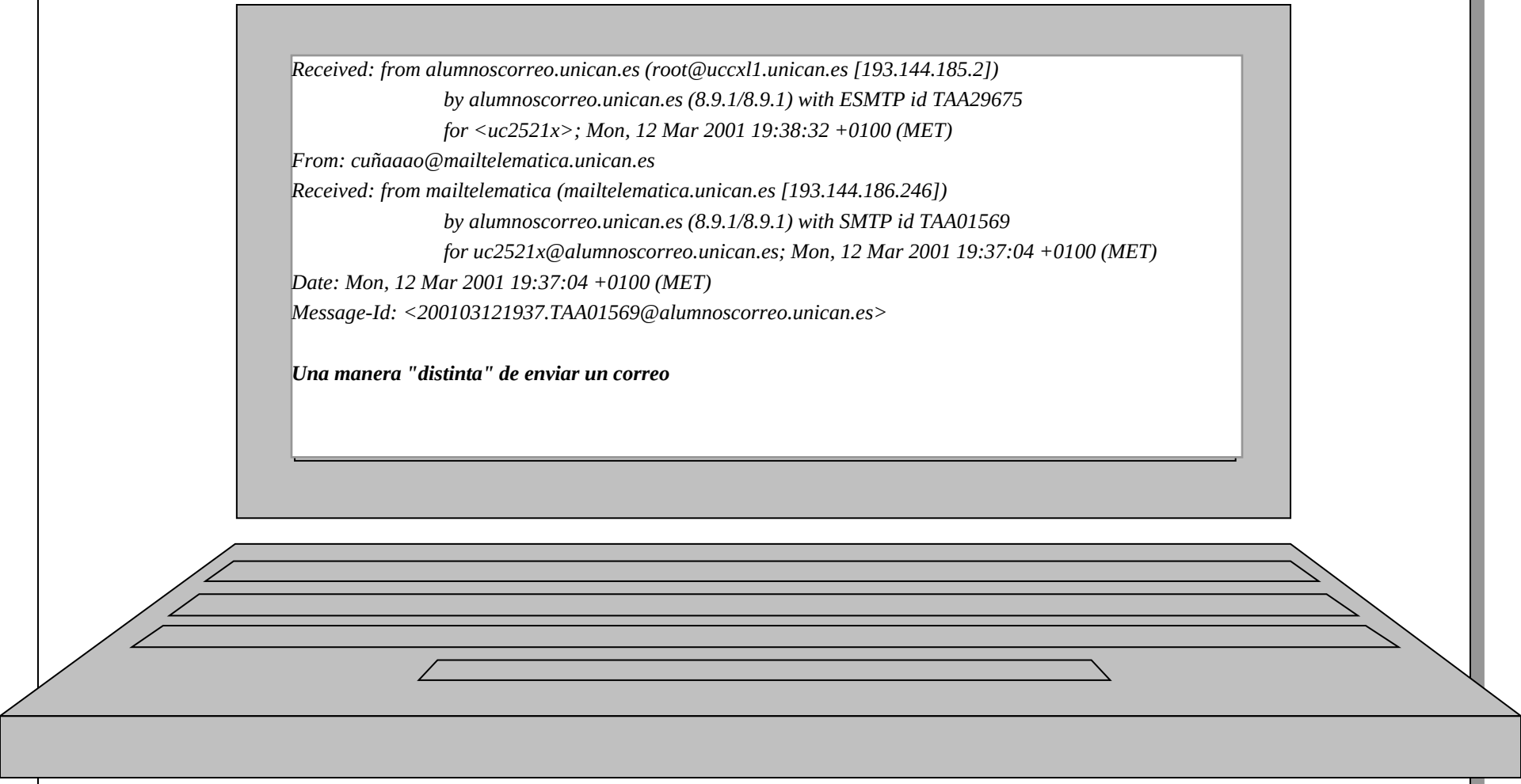
- Usuario: petición de envío de correo
  - Emisor SMTP establece conexión TCP con receptor SMTP (final o intermedio)
- Secuencia de comandos/respuestas
  - Establecimiento del canal: HELO-EHLO
  - Quién envía el mensaje: MAIL/OK
  - Destinatario del mensaje: RCPT/OK
    - Se pueden negociar varios receptores, y sólo se envía una copia del mensaje a un mismo host
  - Envío datos: DATA/OK (secuencia especial de terminación)
  - Cierre del canal: QUIT
  - Otras: verificación de usuario, expansión de listas, envío al terminal

SMTP: comandos

- `HELO cliente`
  - *Inicio sesión SMTP con identificaciones mutuas*
- `MAIL FROM:remitente`
  - *Inicio transacción*
  - *Sobre. Dirección retorno por error.*
- `RCPT TO: destinatario`
  - *Sobre*
  - *Puede repetirse (varios destinatarios)*
  - `250 OK/ 550 Error`
  - `251`*: Destinatario no en servidor, se acepta el mensaje, se retransmite, y se informa de la dirección correcta*
  - `551`*: Ídem sin aceptar mensaje*
- `DATA`
  - *Contenido del mensaje*
  - *Líneas de menos de 1000 bytes*
  - *Final: línea sólo "."*
    - *Remitente: línea que comienza por un punto: añade otro*
    - *Receptor: suprime estos caracteres añadidos*
- `VRFY destinatario`
  - *¿Dirección válida?*
- `EXPN destinatario`
  - *¿Dirección de lista de difusión?*
  - *Miembros de la lista*
  - *En algunos host la diferencia entre listas de correo y alias para un único buzón no está clara*

SMTP: ejemplo de sesión

```
mailtelematica:~> telnet alumnoscorreo smtp
Connected to alumnoscorreo.unican.es.
220 alumnoscorreo.unican.es ESMTP Sendmail 8.9.1/8.9.1 (IRIS 3.0); Mon, 12 Mar 2001
   19:34:22

HELO alumnoscorreo.unican.es
250 alumnoscorreo.unican.es Hello mailtelematica.unican.es [193.144.186.246], pleased
   to meet you

vrfy uc2521x@alumnoscorreo.unican.es
250 PEPITO GRILLO <uc2521x@alumnoscorreo.unican.es>

vrfy errorrr@alumnoscorreo.unican.es
550 errorrr@alumnoscorreo.unican.es... User unknown

mail from: cuñaaao@mailtelematica.unican.es
250 cuñaaao@mailtelematica.unican.es... Sender ok

rcpt to: uc2521x@alumnoscorreo.unican.es
250 uc2521x@alumnoscorreo.unican.es... Recipient ok

data
354 Enter mail, end with "." on a line by itself
Una manera "distinta" de enviar un correo
.
250 TAA01569 Message accepted for delivery
```

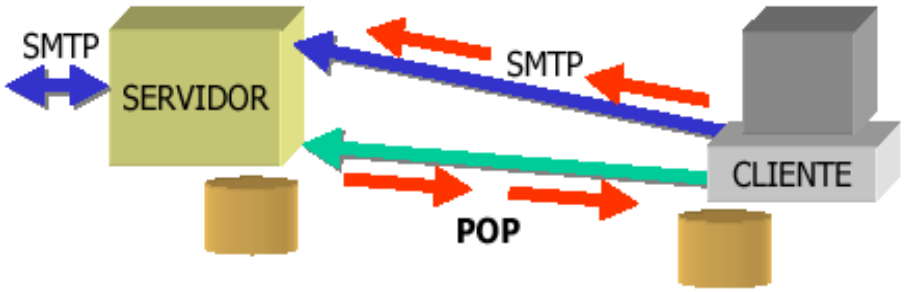

Received: from alumnoscorreo.unican.es (root@uccxl1.unican.es [193.144.185.2])
by alumnoscorreo.unican.es (8.9.1/8.9.1) with ESMTP id TAA29675
for <uc2521x>; Mon, 12 Mar 2001 19:38:32 +0100 (MET)
From: cuñaaao@mailtelematica.unican.es
Received: from mailtelematica (mailtelematica.unican.es [193.144.186.246])
by alumnoscorreo.unican.es (8.9.1/8.9.1) with SMTP id TAA01569
for uc2521x@alumnoscorreo.unican.es; Mon, 12 Mar 2001 19:37:04 +0100 (MET)
Date: Mon, 12 Mar 2001 19:37:04 +0100 (MET)
Message-Id: <200103121937.TAA01569@alumnoscorreo.unican.es>
Una manera "distinta" de enviar un correo

ESMTP

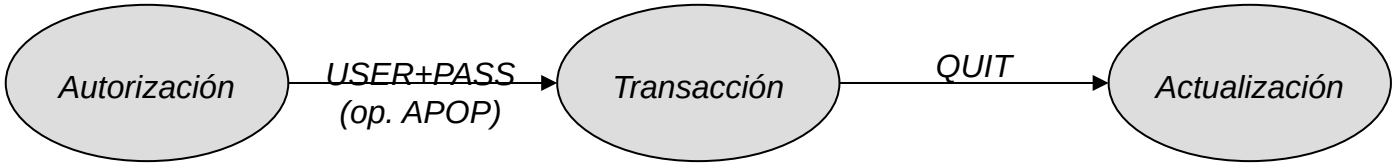
- Limitaciones de SMTP:
  - Codificaciones 7bit, quoted-printable, base64
  - Menos de 100 destinatarios
  - Menos de 1000 caracteres/línea
- Mejoras:
  - *Mensajes con caracteres de 8 bits*
    - `MAIL FROM: remitente BODY=8BITMIME`
    - *ESMTP soporta*
      - *8 bit: caracteres de 8 bits, líneas "cortas" (<1000 bytes)*
      - *Binaria: caracteres 8 bits, sin limitación longitud líneas*
  - *Tamaño de mensajes (RFC 1870)*
    - *Servidor*
      - `250-SIZE 10000000`
    - *Cliente*
      - `MAIL FROM: remitente SIZE=tamaño`
      - *Servidor puede aceptar o rechazar el mensaje*
  - *Autentificación*
    - *Cliente contra el servidor*
    - *Lucha contra spam*
  - *Notificaciones*
    - *Extensión de SMTP*
      - *DSN: Delivery Status Notifications (RFCs 1891-1894)*
    - *SMTP debe notificar incidencias en entrega a uno o más destinatarios*
      - *Mensaje indicando el éxito/fallo*
    - *Con listas: difícil diagnosticar qué destinatario falló*
      - *Mensaje normal en formato libre*
    - *Requisitos*
      - *Fiable: indicación de éxito o fallo en entrega*
      - *Estable: fallo en entrega de DSN no genera DSN*
      - *Informativo: indica transacción y destinatario*
      - *Interoperable: con otros sistemas de correo*
  - *Otras extensiones*
    - *Transporte de binarios: BDAT, CHUNKING*
    - *Envío de mensajes en : ETRN*
    - *Segmentación de comandos: PIPELINING*
      - *Para comunicaciones con gran latencia*
    - *Recuperación de comunicaciones interrumpidas: CHECKPOINT*

Acceso al correo: POP

- Los clientes de correo electrónico en PC se suelen conectar a un servidor de correo cercano (de su proveedor) para enviar mensajes. No se conectan directamente a un servidor remoto al destinatario, o a un servidor con una pasarela a otra red a la que pertenezca el destinatario.
- Los clientes de correo electrónico de PC usan el protocolo POP o IMAP para traer los mensajes entrantes.
- POP3 ≡ Post Office Protocol - Version 3, TCP puerto 110
- RFC 1725
- Acceso de usuario a buzón de correo remoto
  - Autentificación
  - Manipulación
- Recepción de correo en máquinas conectadas eventualmente (receptor iniciador, emisor almacén)
- Comandos ↔ Respuestas
  - (+OK | -ERR)



POP3: Diagrama de estados



AUTHORIZATION

- Identificación de usuario
  - USER uc2521x
  - PASS micontraseña (viaja por la red en claro!!!)
- Identificación más segura: comando APOP (opcional)
  - El servidor emite, junto con el saludo inicial, un sello de tiempo (diferente para cada saludo)

    `<process-id.clock@host>`
  - Sello de tiempo + secreto compartido (conocida por cliente y servidor) → Algoritmo MD5 (RFC 1321) → Cadena de 16 bytes

    `APOP luis cadena_MD5`

TRANSACTION

- Buzón abierto y con acceso exclusivo durante la sesión
- Comandos
  - STAT: número de mensajes y tamaño del buzón
  - LIST [msg]: número y tamaño de cada mensaje
  - RETR msg: solicitud de un mensaje (no marcado para borrar)
  - DELE msg: marca mensaje para eliminarlo
  - RSET: elimina las marcas de borrado
  - TOP msg n: ver cabecera y n líneas de un mensaje (opcional)
  - UIDL msg: solicita identificador único de mensaje (opcional)
  - NOOP: mantiene la conexión activa

UPDATE

- Tras comando QUIT en el estado de transacción
- Libera recursos adquiridos en TRANS
- Se desbloquea el buzón del usuario
- Se eliminan los mensajes marcados para borrar

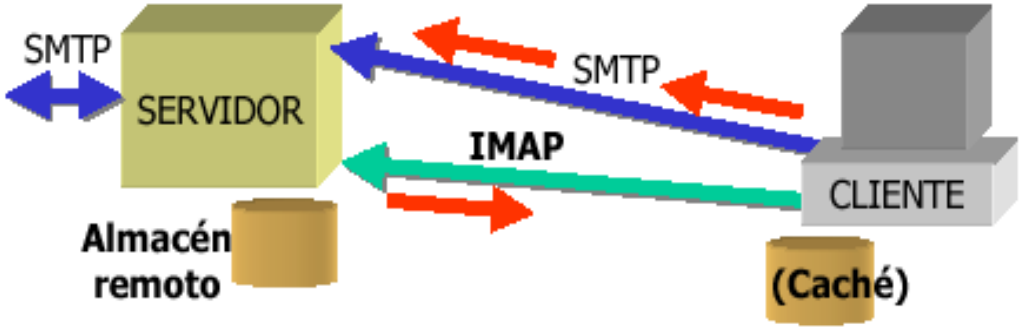
POP3: Ejemplo de sesión

```
S: +OK POP3 server ready <196.671702@dbc.mtview.ca.us>
C: APOP mrose c4c9334bac560ecc979e58001b3e22fb
S: +OK mrose's maildrop has 2 messages (320 octets)
C: STAT
S: +OK 2 320
C: LIST
S: +OK 2 messages (320 octets)
S: 1 120
S: 2 200
S: .
C: RETR 1
S: +OK 120 octets
S: <El servidor POP3 envía el mensaje 1>
S: .
C: DELE 1
S: +OK message 1 deleted
C: RETR 2
S: +OK 200 octets
S: < El servidor POP3 envía el mensaje 2>
S: .
C: DELE 2
S: +OK message 2 deleted
C: QUIT
S: OK server at dbc.mtview.ca.us signing off
```

```
USER mrose
PASS public0
```

Acceso al correo: IMAP

- IMAP4 ≡Internet Message Access Protocol -Version 4rev1
  - Manipulación de almacenes de mensajes remotos
  - Mensajería cliente-servidor
  - Acceso a correo desde varias computadoras
- Necesidad (almacén remoto + protocolo)
  - Uso de más de un computador?, conexiones lentas?
  - Comparto carpetas de correo?, alguien gestiona el almacén?
- RFC 2060 y muchos más
- www.imap.org
- Puerto TCP/143 (asume conexión fiable)



IMAP4: Modos de acceso

- Modos de acceso remoto a buzones de correo:
  - Offline
    - cliente recoge los mensajes del servidor y los borra
    - conexión periódica+transferencia
    - proceso msg local
  - Online
    - mensajes en servidor manipulados por cliente(s) remotos
  - Disconnected
    - cliente se conecta al servidor, realiza una copia (cache) de mensajes seleccionados y se desconecta
    - Reconexión y resincronización
    - proceso msgs local
  - Online y Disconnected

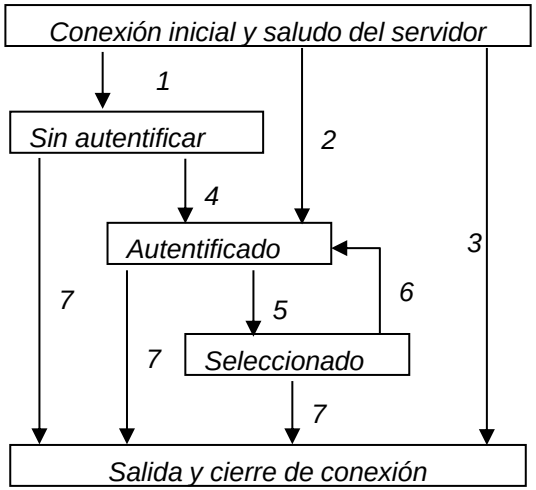
adecuado para usuarios ...

- *POP: bueno para modo "offline"*
  - *Modo "online": alguna funcionalidad (Leave mail on server)*
    - *Pero muchas limitaciones*
      - *Estado de los mensajes local, optimizaciones conectado, ...*
- *IMAP*
  - *Muchas ventajas respecto POP*
  - *Desventajas*
    - *Complejidad*
    - *Menos implementaciones sw*

- Manipulación remota de buzones
  - Añadir mensajes
  - Marcas en mensajes
  - Notificación de nuevos correos
  - Acceso concurrente/compartido a carpetas
- Soporte de múltiples buzones
  - Acceso a múltiples buzones (nombres UTF-7), servidores
  - Crear, borrar, renombrar buzones remotos
  - Jerarquías de carpetas
- Optimización de prestaciones conectado (on-line)
  - Estructura del mensaje sin transferirlo
  - Acceso selectivo a partes MIME de un mensaje (anexos…)
  - Búsqueda y selección por el servidor
- Autentificación avanzada (similar a POP) [sasl]
- Protocolo extensible

IMAP4: Diagrama de estados

- Conexión IMAP
  - Establecimiento conexión
  - Saludo del servidor
  - Interacciones cliente/servidor
    - Comandos del cliente
    - Datos del servidor
    - Respuestas de finalización de operación (S)
    - Líneas acabadas en <CRLF>



1. Conexión sin pre autentificación
2. Conexión pre autentificada (por medios externos)
3. Conexión rechazada
4. Tras LOGIN o AUTHENTICATE correcto
5. Tras SELECT/EXAMINE
6. Después de CLOSE o por SELECT/EXAMINE fallido
7. LOGOUT, cierre de la conexión, parada del servidor

Seguridad en IMAP4

- Todas las transacciones (contraseñas, mensajes de correo, ...) se transmiten en claro, a menos que se negocie una protección con el comando AUTHENTICATE
- Mensajes de error del servidor;
  - Por comandos AUTHENTICATE fallidos: no deben detallar las causas del error
  - Por comandos LOGIN fallidos: no deben especificar si erróneo el nombre de usuario o el password
- LOGIN usuario password se envía en claro

News vs Listas correo

- Listas
  - Paradigma “push” (usuario pasivo)
  - Envío de copia a cada destinatario
  - Mantenimiento lista
  - Envío a distintos destinatarios

- News
  - Paradigma “pull” (usuario activo)
  - Mensajes almacenados en BD central
  - Consulta de mensajes interesantes
  - Indexación, referencias cruzadas, eliminación por tiempo

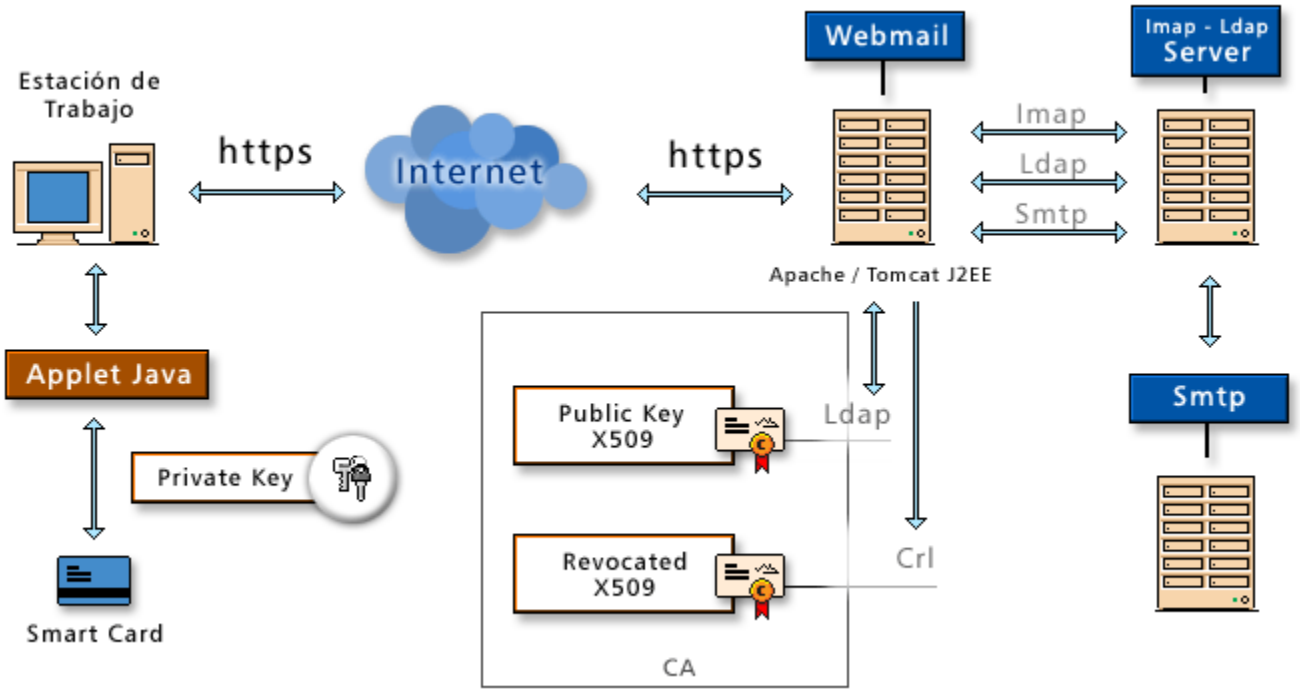
News vs Listas correo

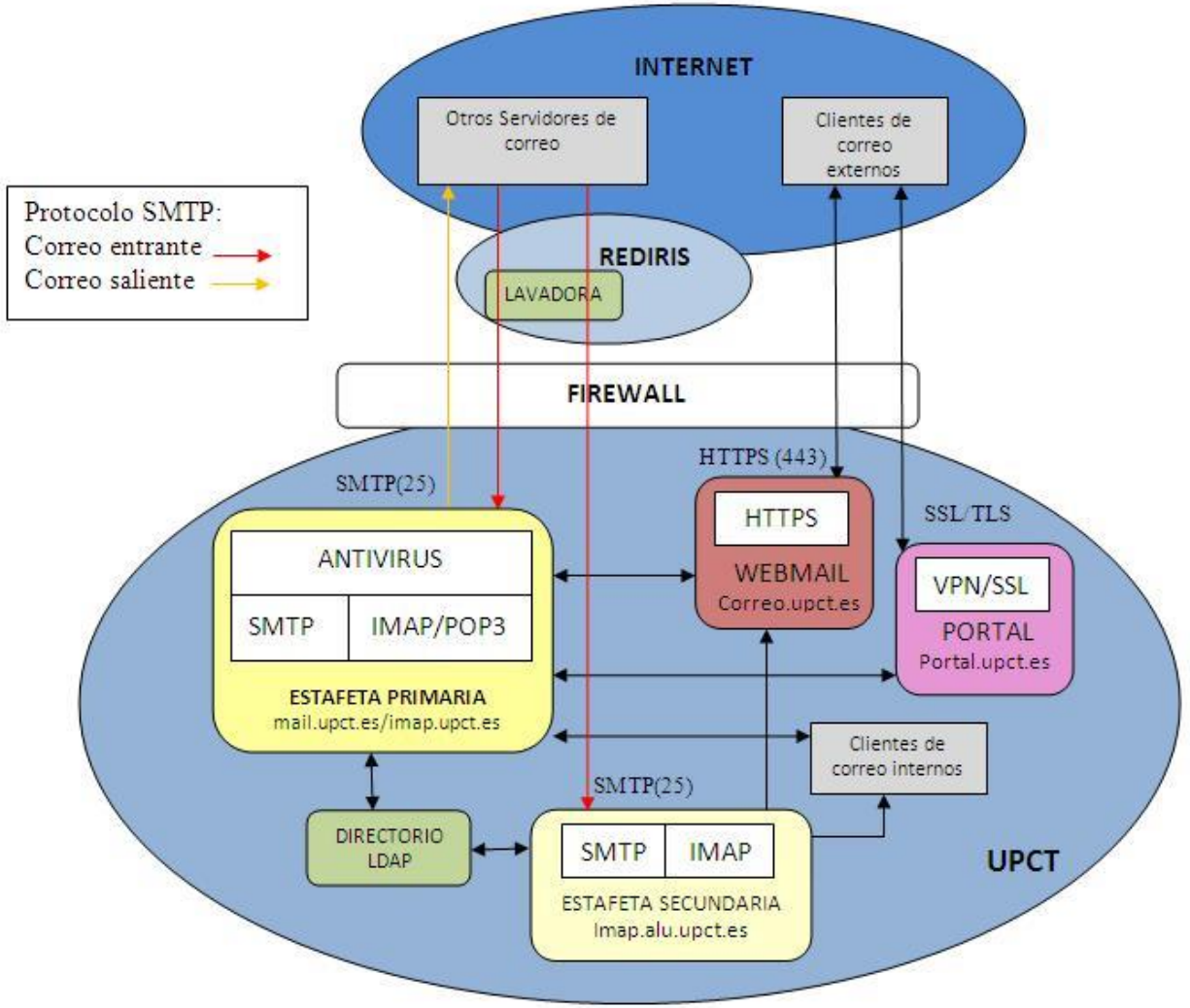
- Ventajas listas correo
  - Control de aportaciones
  - Conocimiento destinatarios
  - Posibilidad de optimizar carga buzones (DIGEST, ...)
  - Herramientas anti-spam
  - Algoritmos optimización tráfico internacional

- Ventajas news
  - Gestión centralizada
  - Origen histórico de las FAQs
  - Usuarios potenciales = todos usuarios Internet

Webmail

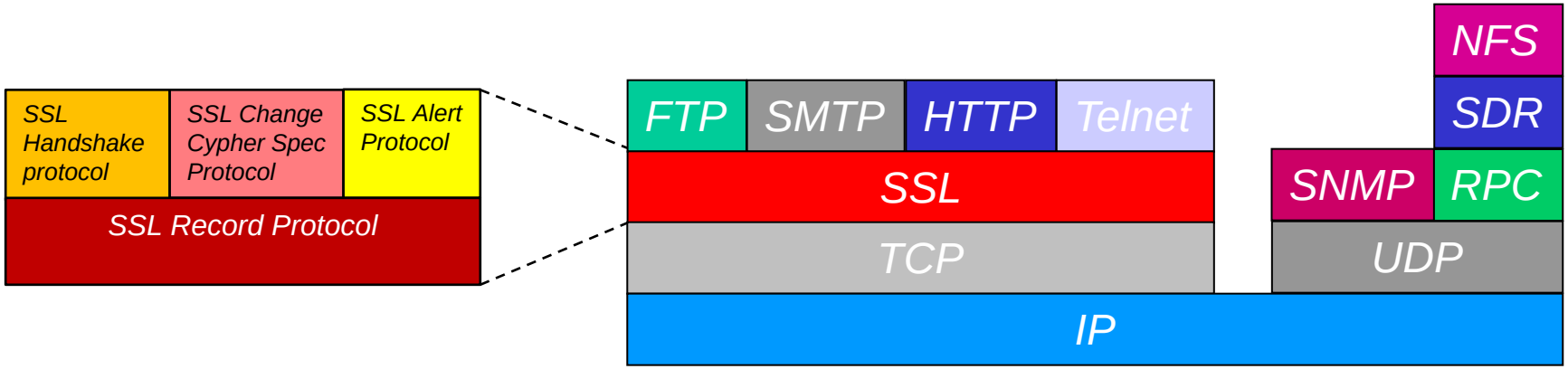
- Un **correo web** es un cliente de correo electrónico, que provee una interfaz web por la que acceder al correo electrónico.



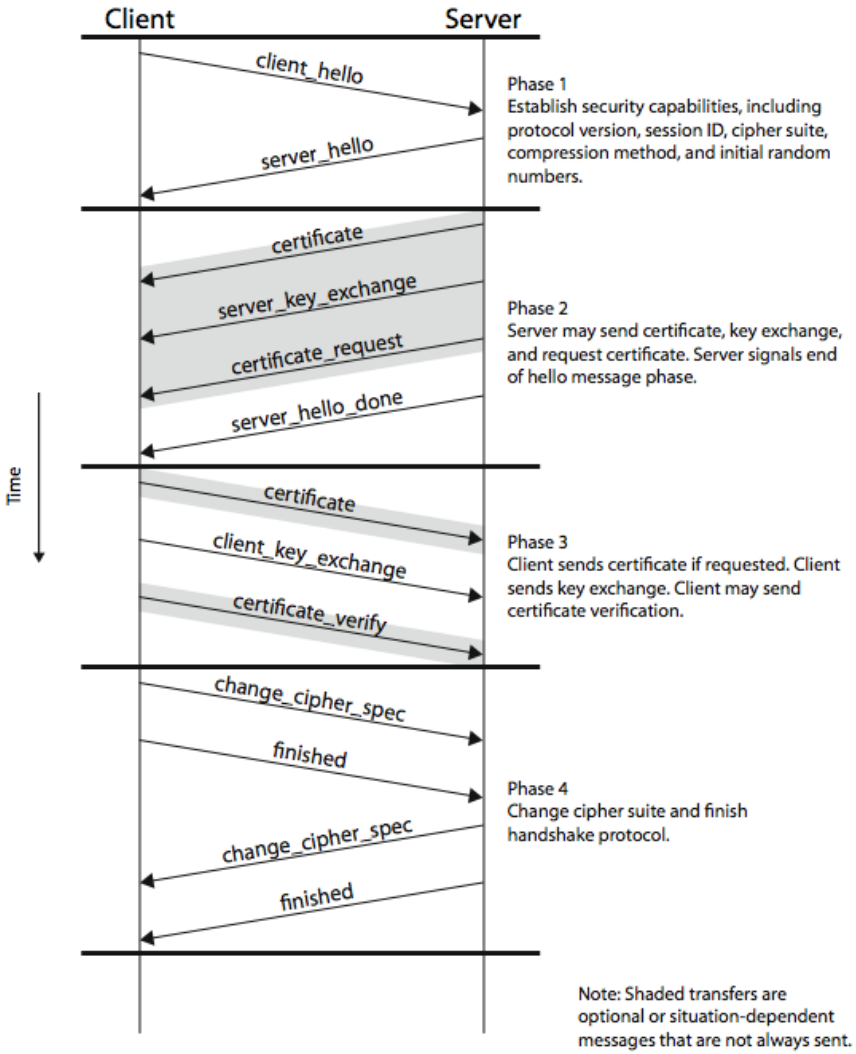

INTERNET
Otros Servidores de correo
Clientes de correo externos
REDIRIS
LAVADORA
Protocolo SMTP:
Correo entrante
Correo saliente
FIREWALL
HTTPS (443)
SMTP(25)
SSL/TLS
HTTPS
WEBMAIL
Correo.upct.es
ANTIVIRUS
SMTP
IMAP/POP3
ESTAFETA PRIMARIA
mail.upct.es/imap.upct.es
VPN/SSL
PORTAL
Portal.upct.es
Clientes de correo internos
SMTP(25)
DIRECTORIO LDAP
SMTP
IMAP
ESTAFETA SECUNDARIA
Imap.alu.upct.es
UPCT

Protocolos seguros: SSL *(Secure Socket Layer)*

- Protocolo de propósito general para el envío de información cifrada
- Aparece en 1994 (*Netscape)*
- El IETF definió el TLS *(Transport Layer Security*) basado en la V. 3.0
- WTLS es la variante en entornos wireless
- No aparece sobre UDP: *SSL es un protocolo orientado a la **conexión***
- No protege SNMP, RPC, NFS, DNS ....

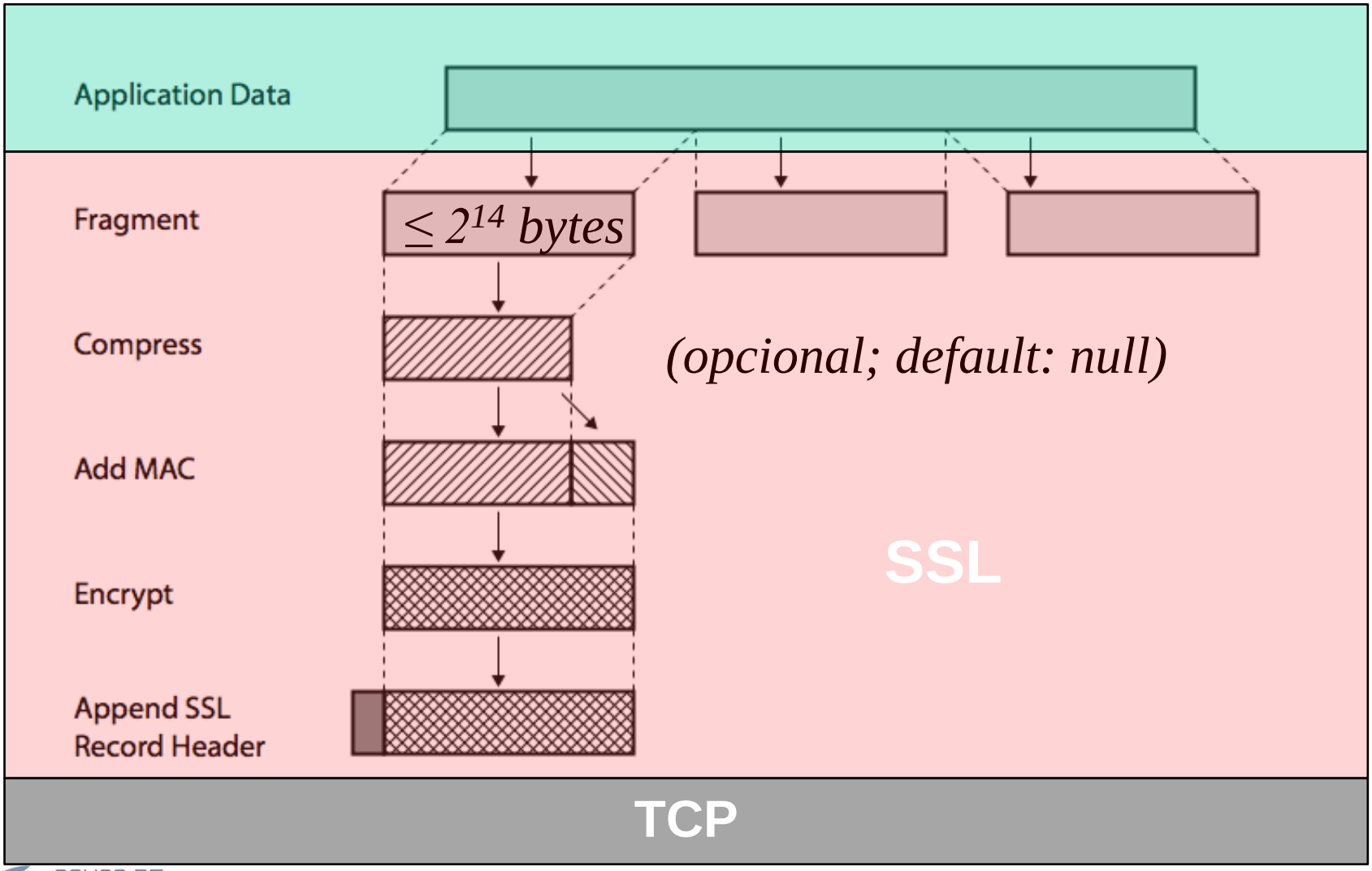


SSL: Establecimiento de una sesión segura



Fuente: Stallings

SSL: Fragmentación/Compresión/Encriptación



SSL: Puertos seguros

- Hay puertos IP específicos para la comunicación aplicación – SSL

Protocolo Seguro	Puerto	Aplicación
HTTPS	443	HTTP
SSMTP	465	SMTP
SNNTP	536	NNTP
SPOP3	995	POP3
SSL-LDAP	636	LDAP

Protocolo Seguro	Puerto	Aplicación
FTP-DATA	889	FTP
FTPS	990	FTP
IMAPS	991	IMAP4
IRCS	993	IRC
TELNETS	992	Telnet

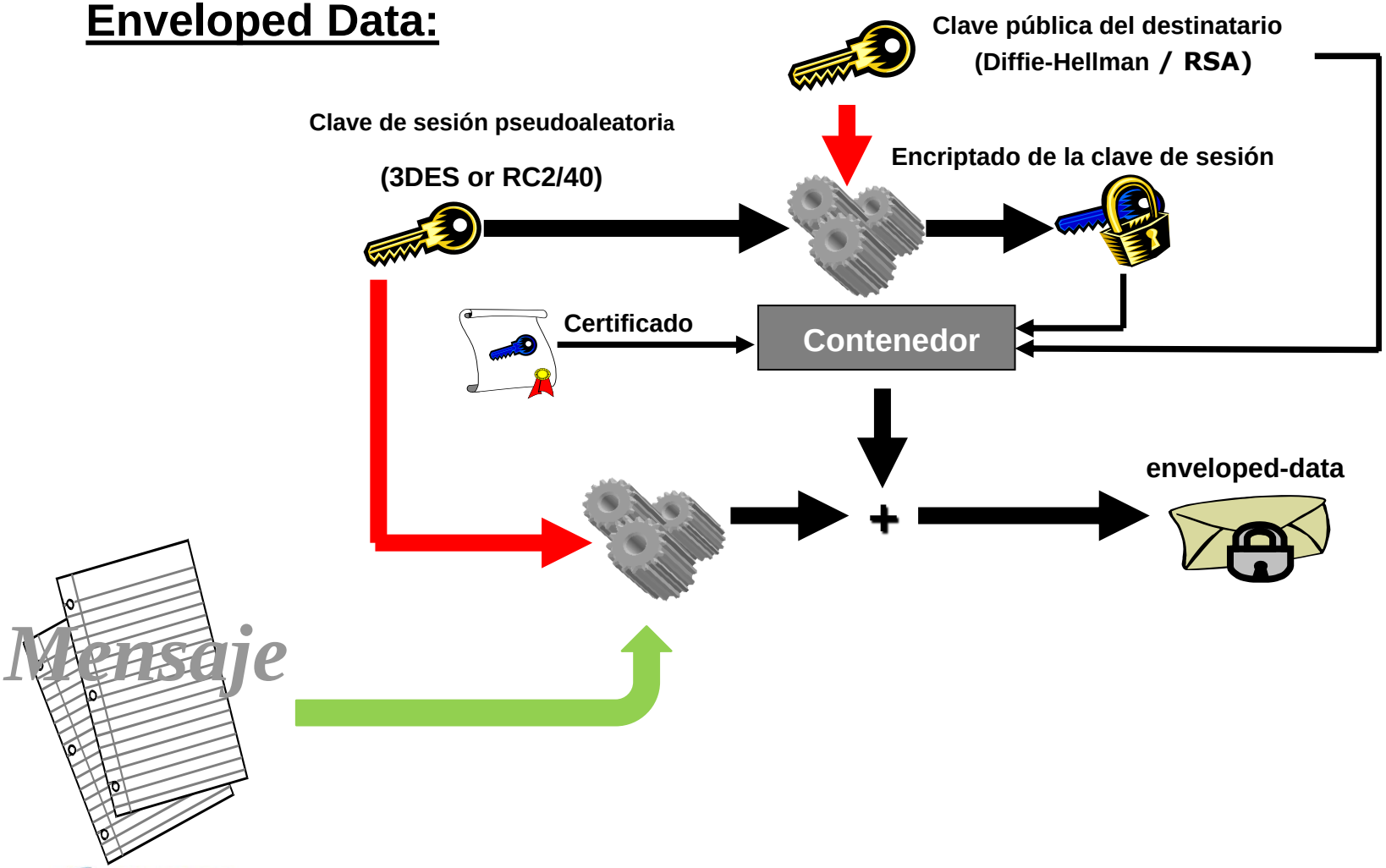
SSMTP: Secure Simple Mail Transfer Protocol
NNTP: Network News Transfer Protocol
LDAP: Lightweight Directory Access Protocol
POP: Post Office Protocol
IMAP: Internet Message Access Protocol
IRC: Internet Relay Chat

SSL:Correo seguro (S-MIME)

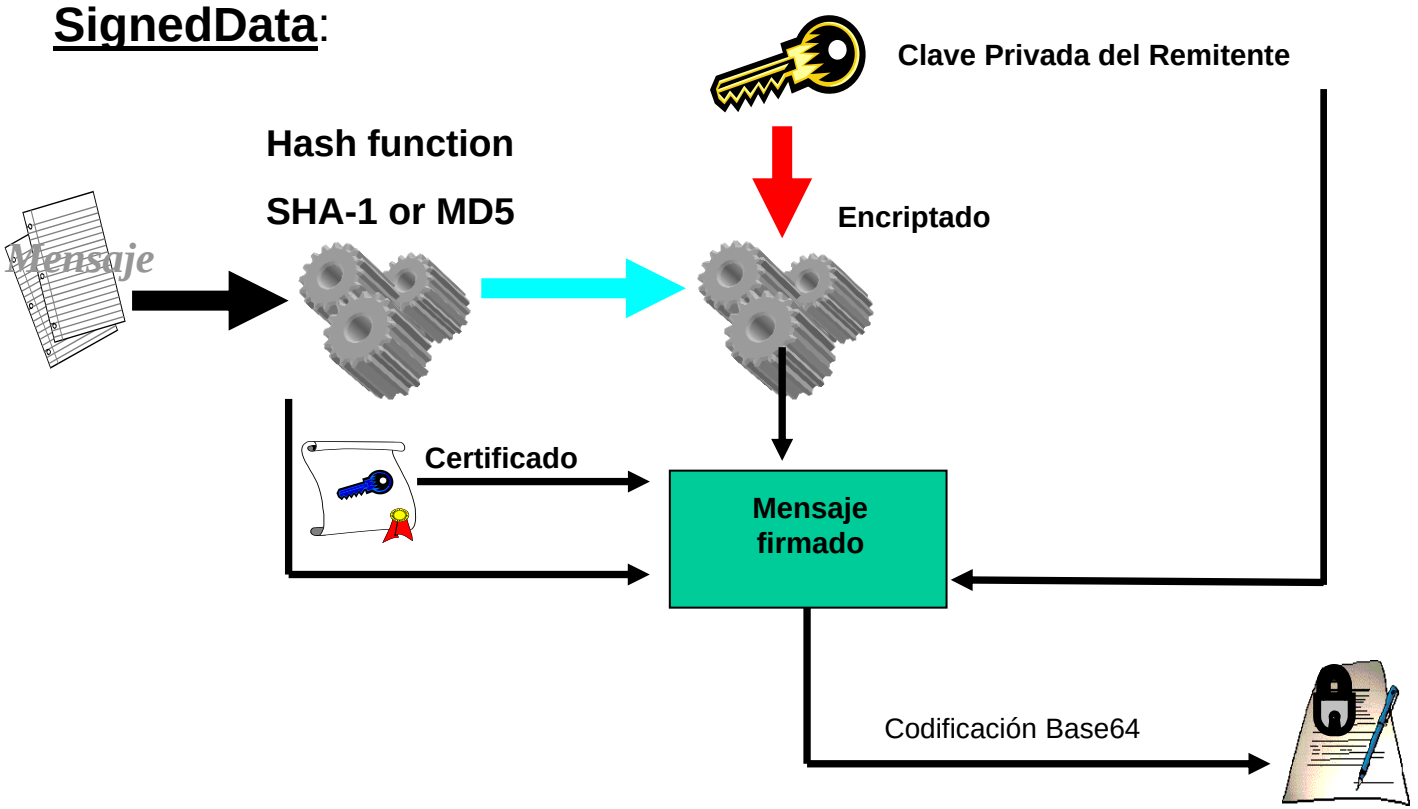
- MIME *(Multipurpose Internet Mail Extension)*
  - firmas digitales y cifrado
  - Cifrado simétrico:RC2, RC5, DES y Triple DES
  - Cifrado asimétrico: RSA
  - Funciones de mezcla: SHA-1,
- Requiere el uso de certificados digitales X.509
- Adoptado por Netscape, Microsoft, Lotus, Novell, Verisign, etc.
- Actualmente se encuentra en fase de estandarización por el IETF

S-MIME: Datos seguros

Enveloped Data:



S-MIME: Datos firmados



Servicios de DIRECTORIO

- Identifican todos los recursos de una red
  - Direcciones de correo, computadores, impresoras, ...
- Los hace accesibles a usuarios y aplicaciones
- Oculta topología y protocolos
  - Acceso a recursos sin tener que saber dónde, cómo están conectados
- Ejemplos:
  - X.500: servicio de directorio OSI
  - LDAP: Lightweight Directory Access Protocol
  - Whois (DNS), Whois++
  - Netware Directory Service (NDS)

Servicios de Directorio: Funciones

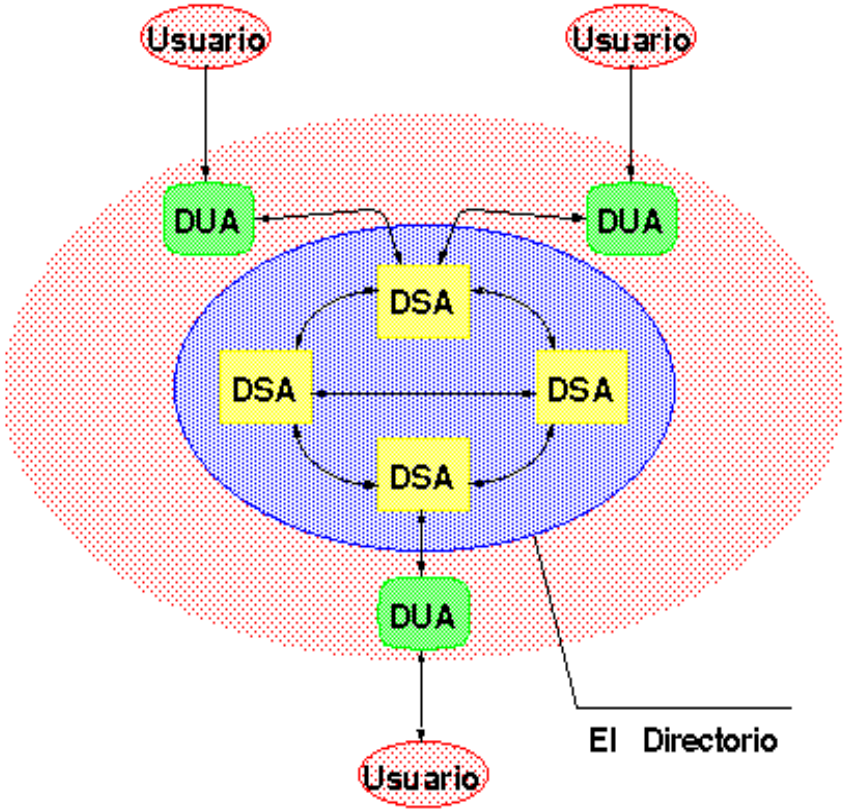
- Búsqueda de direcciones de personas y organizaciones
  - BD distribuida universal (aparentemente centralizada)
  - X.500, LDAP, Whois++
- Info almacenada en directorios
  - Nombre, dirección correo, teléfono, fax, dirección postal, ...
  - Servicios criptográficos
    - Certificados criptográficos (servidor de certificados)
    - Identificación, autorización, firmas, pagos, ... (canales seguros –SSL-)

Servicios de Directorio: X.500

- Servicio de directorio global
- Directorio OSI
- Especificaciones en 1988. Extendido en 1993
- BD distribuida entre muchos servidores
- DIB - Base de Información del directorio
  - Información contenida en el directorio
  - Objetos: personas, organizaciones, aplicaciones

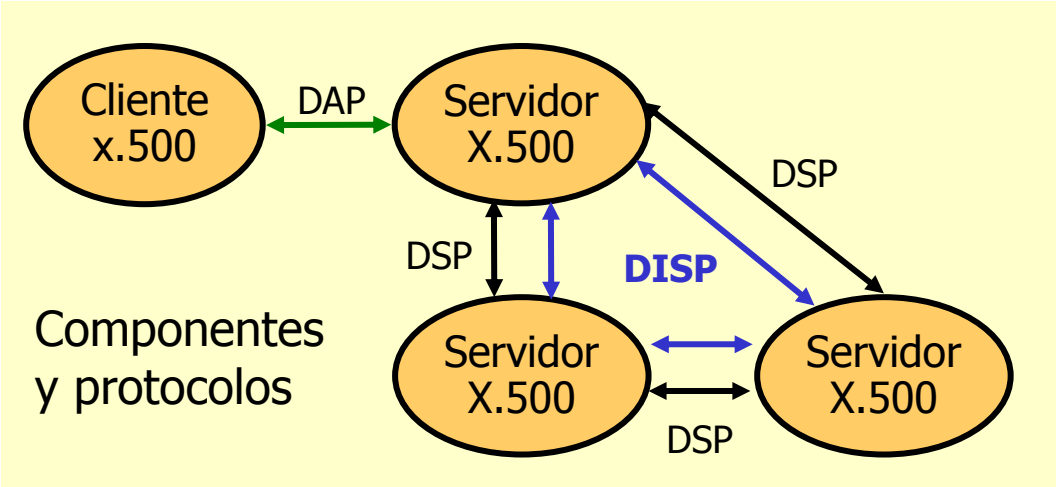
X.500: Arquitectura

- DSAs – Agentes de Sistema de Directorio
  - Mantiene la info distribuida del directorio
  - BD local
  - Procedimientos de comunicaciones para diálogo entre:
    - DSAs: DSP
    - DSA-DUAs (Agentes de Usuario de Directorio): DAP



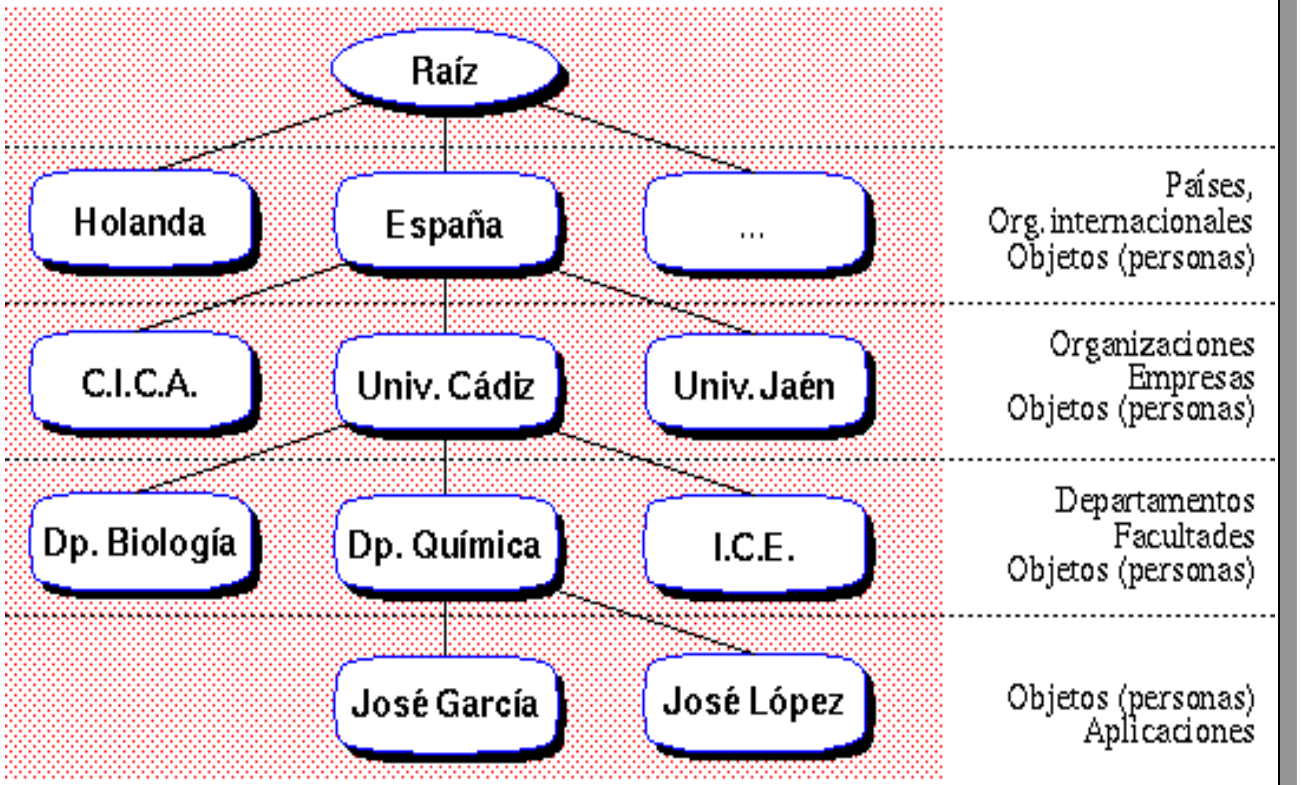
X.500: Protocolos

- DAP: Directory Access Protocol (capa superior pila OSI)
- DSP: Directory System Protocol
- DISP: Directory Information **Shadowing** Protocol
- DUA: Directory User Agent (cliente, DAP con servidor)
- DSA: Directory Server Agent (servidor, DAP con clientes, DSP y DISP con otros servidores)



X.500: Estructura del Directorio

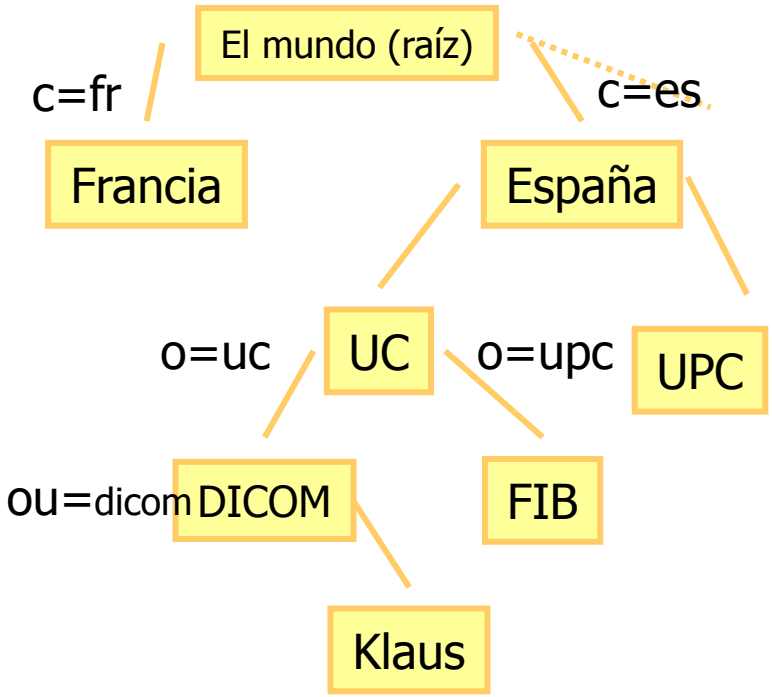
- DIT: Árbol de Información del Directorio
  - Búsquedas rápidas y sencillas
- Jerárquica en niveles (origen en raíz)
- Un encargado de mantenimiento por nivel



X.500: Entradas del Directorio

- Objetos = Nombre + atributos
- Nombre único objetos: DN – Nombre distintivo
- Atributos: país (c), organización (o), unidad de organización (ou), nombre del objeto (cn), otras propiedades.
- RDN: Nombres Distintivos Relativos
- DN = Secuencia RDN (desde raíz)

  DN: "@c=ES @o=Universidad de Cantabria
  @ou= Dpto. Ingeniería de Comunicaciones
  @cn= Klaus Hackbarth"
  RDN 1: c=ES
  RDN 2: o= Universidad de Cantabria
  RDN 3: ou= Dpto. Ingeniería de Comunicaciones
  RDN 4: cn= Klaus Hackbarth
- Operaciones DUAs
  - Añadir, borrar, modificar entradas
  - Lectura, listado, búsqueda de objetos



X.500: Aplicaciones

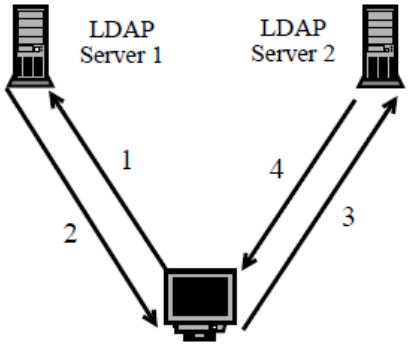
- Interpersonales: usuario-directorio
  - Páginas blancas: búsqueda por nombre (DN y atributos del objeto buscado)
    - Ej: personal del departamento de Informática de la UC
  - Páginas amarillas: búsqueda por atributos
    - Ej: personal del departamento de Informática de la UC que se llame Klaus
- Entre sistemas: aplicaciones OSI-directorio
  - Directorio selecciona aplicación que realiza servicio deseado
  - FTAM: transferencia, acceso y gestión de ficheros distribuidos

Servicios de Directorio: LDAP

- Lightweight Directory Access Protocol
  - LDAP v2: RFC 1777
  - LDAP v3: RFC 2251
- Protocolos para el acceso a directorios de información globales
  - Visión del directorio independiente del servidor
- Basado en X.500, pero más simple y con soporte TCP/IP
  - TCP puerto 389
  - SSL puerto 636
- Obtención
  - Direcciones correo
  - Claves públicas

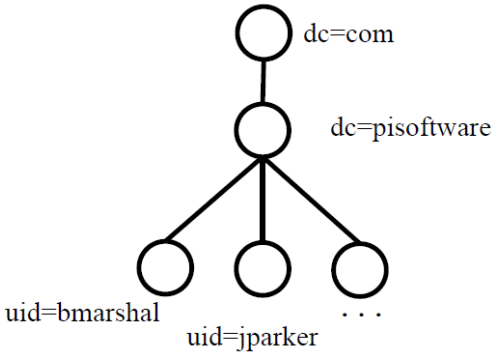
LDAP: Características

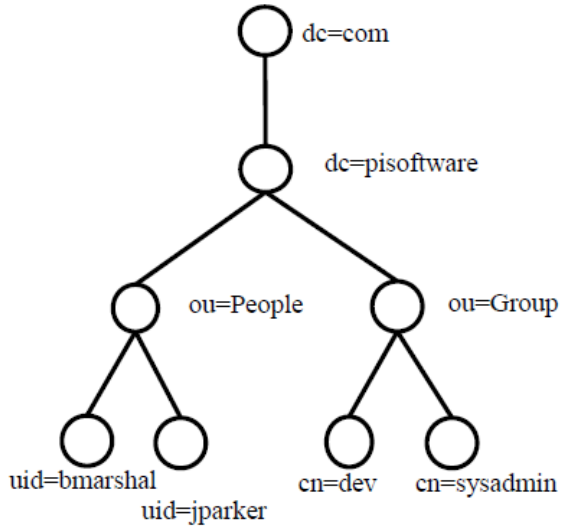
- Información en el directorio
  - Entradas = colección de atributos con tipo y valor/es con un nombre distinguido (DN)
- Estructura
  - Jerárquica en forma de árbol
- Referencia
  - Por nombre distinguido (DN)
- Acceso a información
  - Consultas y actualización del directorio
- Control de acceso
  - Protección de info: autentificación
    - Anónima, simple (pwd en claro), Kerberos v4
    - SSL (LDAPv3)
- Modelo cliente-servidor
  - Pregunta cliente
  - Respuesta servidor
    - Info demandada
    - Puntero a otra fuente de info (v3)
- TCP o UDP (v3)

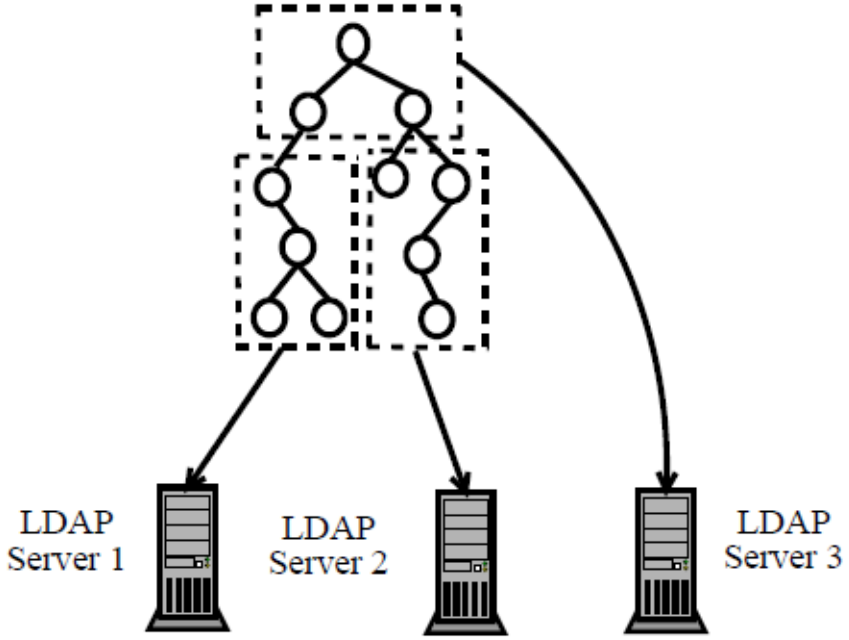


1. Cliente hace una petición
2. Server 1 devuelve una referencia a Server 2
3. Cliente reenvía la petición a Server 2
4. Server 2 devuelve la información a Cliente

LDAP: Estructura del directorio

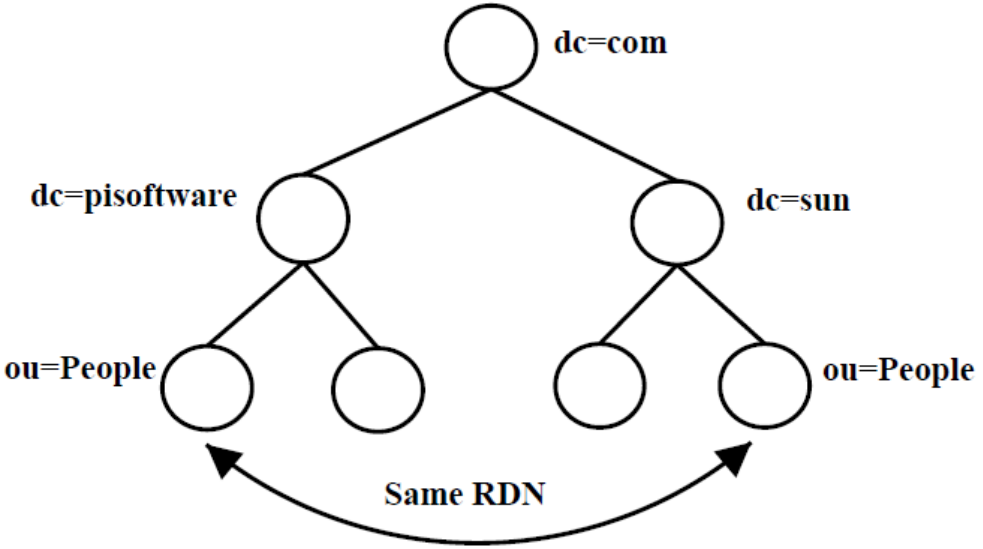






LDAP: Nombres Distinguidos

- Utiliza el nombre DNS para generar el DN
- RFC2377 - "Naming Plan for Internet Directory-Enabled Applications"
  - example.com -> dc=example,dc=com
- Asegura un nombre único global
  - El nombre ya está así registrado y asegura su trazabilidad



LDAP: Esquema

- Conjunto de reglas que describen cómo se almacenan los datos (ASN.1)
- Ayuda a mantener la consistencia y calidad de los datos
- Reduce los duplicados
- Asegura una interface consistente a las aplicaciones
- Los atributos de la Clase Objeto determinan el Esquema que cualquier nuevo conjunto de datos deben seguir

Ejemplos de Atributos (RFC2256)

uid *User id*
cn *Common Name*
sn *Surname*
l *Location*

ou *Organisational Unit*
o *Organisation*
dc *Domain Component*
st *State*
c *Country*

- **Cada Esquema incluye:**
  - Atributos obligatorios
  - Atributos permitidos
  - Cómo comparar atributos
  - Tipos de datos y sus límites de almacenamiento
  - Restricciones para los datos permitidos
- **Cada Clase Objeto incluye:**
  - Reglas para datos requeridos y datos permitidos
  - Puede proceder de una sola Clase Objeto de la que hereda todos sus atributos
- **Cada atributo incluye:**
  - Name: único
  - OID: Identificador, secuencia de enteros separados por puntos
  - Syntax: Tipo de datos y operaciones de comparación
  - Single/Multi: uno o varios valores

LDAP: LDIF

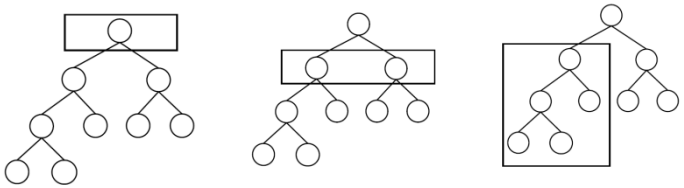
- LDAP Data Interchange Format
  - Representación textual de la entradas LDAP
  - Formato legible
  - Permite modificar de forma sencilla los datos
  - Util para cambios voluminosos
    - Capturar base de datos, ejecutar scripts, reimportar
  - Permite el uso de templates
  - Util para backups y exportación

```
dn: uid=bmarshal,ou=People,
dc=pisoftware,dc=com
uid: bmarshal
cn: Brad Marshall
objectclass: account
objectclass: posixAccount
objectclass: top
loginshell: /bin/bash
uidnumber: 500
gidnumber: 120
homedirectory: /mnt/home/bmarshal
gecos: Brad Marshall,,,,
userpassword: {crypt}KDnOoUYN7Neac
```

LDAP: Búsqueda en el directorio

- Se permite especificar criterios concretos por atributos
- Stándares:
  - RFC 1960: LDAP String Representation of Search Filters
  - RFC 2254: LDAPv3 Search Filters
- Operadores:
  - & and
  - | or
  - ! not
  - ~= approx equal
  - >= greater than or equal
  - <= less than or equal
  - * any

Scope: *Base* *One level* *Subtree*



```
dn: uid=bmarshal,ou=People,
dc=pisoftware,dc=com
uid: bmarshal
cn: Brad Marshall
objectclass: account
objectclass: posixAccount
objectclass: top
loginshell: /bin/bash
uidnumber: 500
gidnumber: 120
homedirectory: /mnt/home/bmarshal
gecos: Brad Marshall,,,,
userpassword: {crypt}KDnOoUYN7Neac
```

Ejemplos:

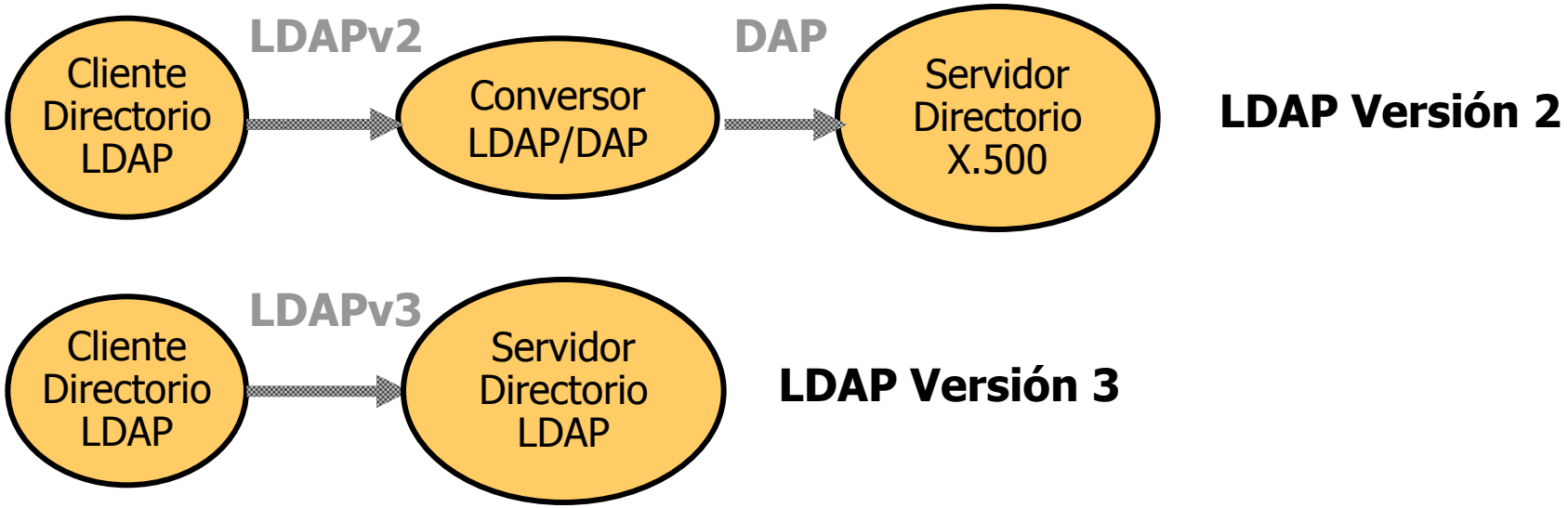
```
(objectclass=posixAccount)
(cn=Mickey M*)
(|(uid=fred)(uid=bill))
(&(|(uid=jack)(uid=jill))(objectclass=posixAccount))
```

LDAP: Operaciones

- bind: conexión y autentificación
- unbind: desconexión
- search: búsqueda
- modify / add / delete: modificar / añadir / eliminar una entrada
- modify RDN
- compare: comprobar si una entrada tiene un pareja atributo/valor
- abandon: cancelar una petición pendiente

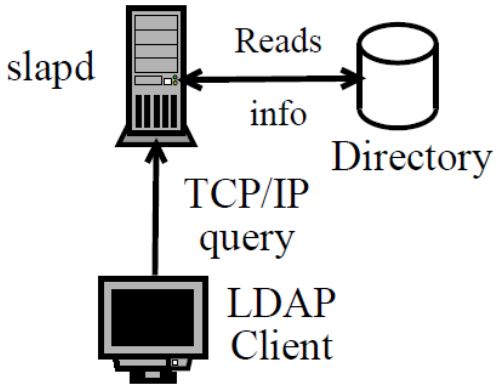
LDAP: LDAPv3

- El servidor (ldapd) no necesita X.500
- Internacionalización: ISO 10646, UTF-8
- Autentificación: SASL (Simple Authentication Security Layer)
  - DIGEST-MD5, CRAM-MD5, S/Key, GSSAPI, Kerberos v4, anónimo, externa

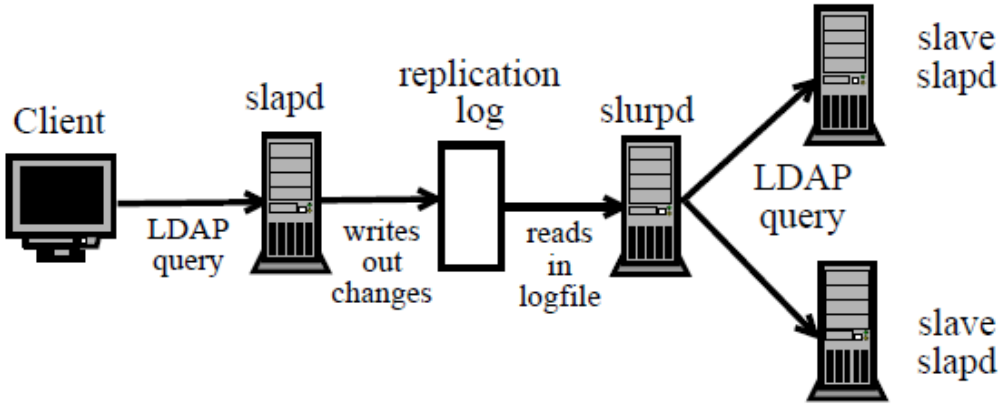


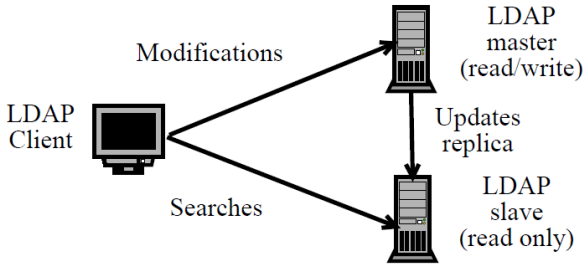
LDAP: Modos de funcionamiento

Sin respaldo



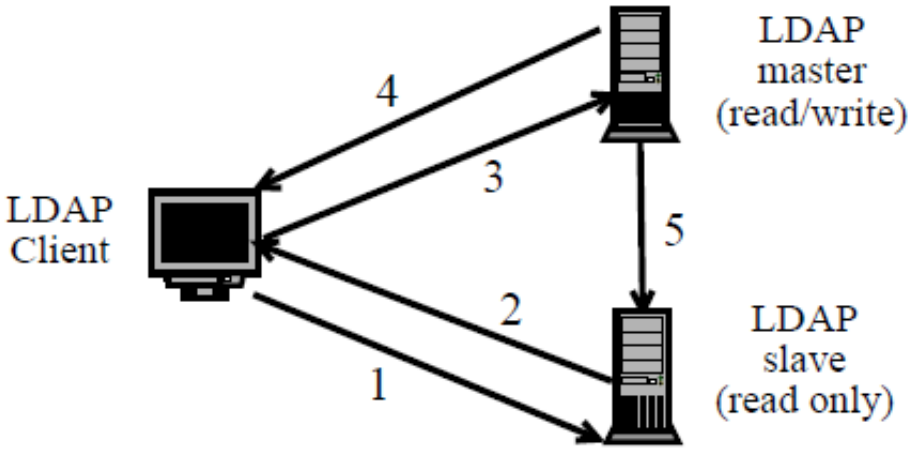
Con respaldo



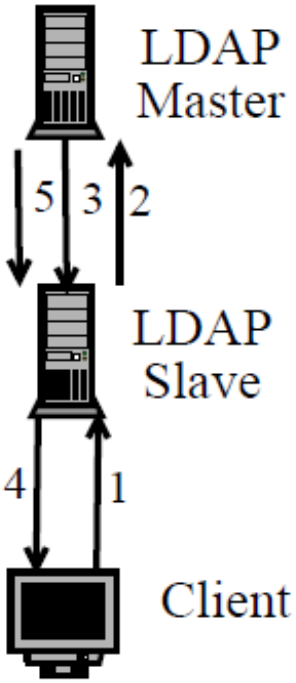


LDAP: Actualizaciones

Por referencia (Referral)



Encadenada (Chaining)



LDAP: Relación con servicios Internet

- Relación con DNS: IDEA “Domain Component” (dn)
  - RDN: uid=leandro@upc.es (buzón correo rfc822)
  - DN: uid=leandro@upc.es,dc=ac, dc=upc, dc=es
  - DN: cn=Biblioteca BGF, dc=upc, dc=es
- Relación con web: ldap URL
  - **ldap://<host:port>/ DN ? Attribute list ? Scope ? Filter**
    - ldap:///o=UPC,c=ES
    - ldap://ldap.upc.es/o=UPC,c=ES
    - ldap://ldap.upc.es/o=UPC,ou=AC,c=ES?mail
    - ldap://foo.bar.com/dc=bar,dc=com
    - ldap://argle.bargle.com/dc=bar,dc=com??sub?uid=barney
    - ldap://ldap.bedrock.com/dc=bar,dc=com?cn?sub?uid=barney
- Relación con correo: vCard (mime)
  - Transporte de info de directorio: sobre correo…

LDAP: Aplicaciones

- Servidores de directorio públicos
  - OpenLDAP, Eudora LDAP Directory Server, The JavaLDAP Server Project
- Servidores de directorio comerciales:
  - M-Vault, Netscape Directory Server, Microsoft ActiveDirectory, ...

- http://www.rediris.es/sdir/software/
  - Servidores de directorio
  - Clientes
  - Pasarelas X500-LDAP
  - Pasarelas Web-LDAP

LDAP vs X.500

- En común:
  - DIT, DNs, atributos, búsquedas por filtros, ...
- X.500: DAP: protocolo de acceso a directorios
  - Especificación muy detallada
  - Sobre OSI
  - Muchos recursos (“pesado”)
- LDAP: acceso ligero a X.500
  - TCP/IP
  - Clientes sencillos
- El directorio X.500 ha llegado a unas 1,5 M. Entradas (9/1998)
  - Crecimiento mucho menor que el de Internet
- Faltan autoridades de registro internacionales:
  - “Organization” (o) deben estar registrados.

Servicios de Directorio: ACAP

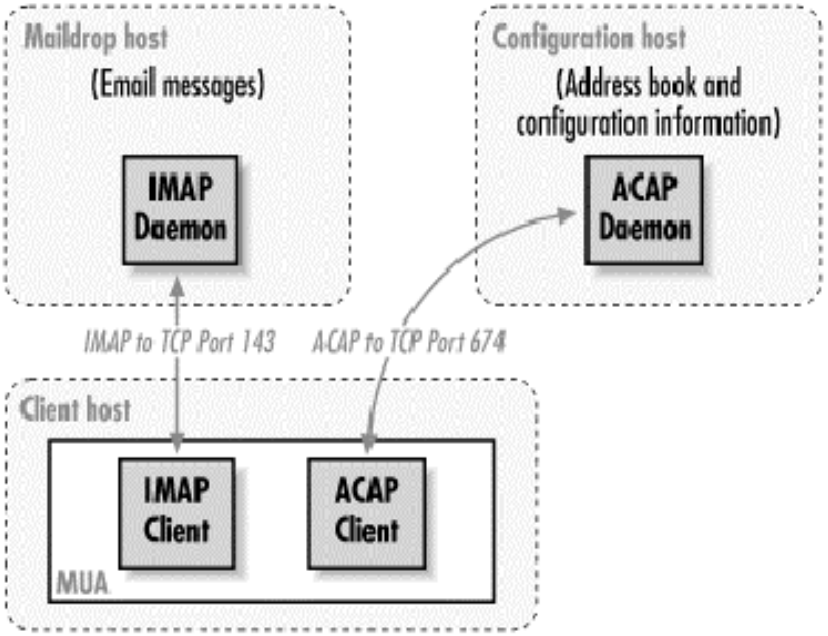
- Application Configuration Access Protocol
- Protocolo derivado de IMAPv4
- Almacenamiento y acceso remoto de información:
  - Preferencias/opciones de configuración de aplicaciones
    - Configuración correo, ...
  - Datos personales
    - Listas de direcciones de correo, diccionarios, bookmarks, listas de subscripción (News), ...
  - Perfiles de usuarios móviles (roaming)
    - N puntos de acceso x N usuarios
- Enfocado a aplicaciones clientes de Internet

ACAP: Descripción

- Motivado por evolución Internet
  - Acceso desde trabajo, casa, viajes, ...
  - Varios usuarios/máquina
  - Varias máquinas/usuario
- No es un servicio de directorio
- Protocolo cliente-servidor
- Comandos del cliente - respuestas del servidor
- Sintaxis y estructura similar a IMAP4
- Conjuntos de datos predefinidos
  - Listas, listas de @ de correo, bookmarks, ...

ACAP: Arquitectura

- Almacenamiento de conjuntos atributo/valor en un servidor



ACAP vs. Servicios de Directorio

- Servicios de directorio (LDAP, X.500, ...)
  - Control del servidor
  - Búsqueda rápida de información pública y “cuasi-estática”
  - Funcionamiento on-line
- ACAP
  - Control del cliente/usuario
  - Datos más dinámicos
  - Funcionamiento off-line (cache-local)