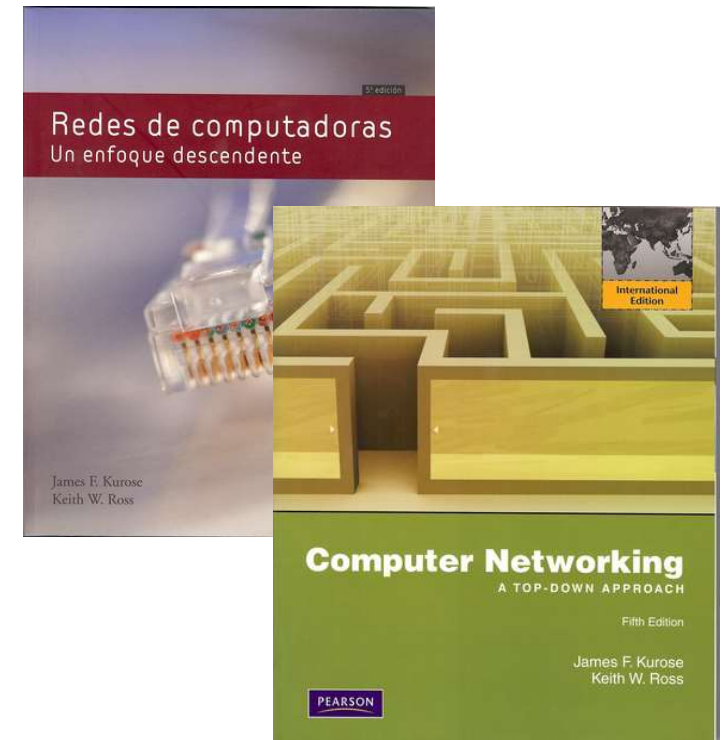




DT^e.
Departamento de
Tecnología Electrónica



*Algunas de las transparencias
tienen copyright:*

*Redes de computadoras:
Un enfoque descendente
5th edition.*

*Jim Kurose, Keith Ross
Addison-Wesley, Abril
2009.*

Capítulo 2

Servicios en red

Capítulo 2: Servicios en red

□ Objetivos del capítulo:

- Entender algunos de los servicios de datos más comunes en las redes de computadores:
 - o Servicios de transferencia de archivos
 - o Servicios de correo electrónico
 - o Servidores de Nombres de Dominio (DNS)

Capítulo 2: Servicios en red

- ❑ 1.1 Introducción
- ❑ 1.2 Servicios de transferencia de archivos
 - TFTP
 - FTP
- ❑ 1.3 Servicios de correo electrónico
 - SMTP
 - POP3
- ❑ 1.4 Servicios de Nombres de Dominio (DNS)

Capítulo 2: Servicios en red

❑ 1.1 Introducción

❑ 1.2 Servicios de transferencia de archivos

- TFTP
- FTP

❑ 1.3 Servicios de correo electrónico

- SMTP
- POP3

❑ 1.4 Servicios de Nombres de Dominio (DNS)

Introducción

- ❑ Servicios en red -> clave en empresas y organizaciones
- ❑ El trabajo está basado en la compartición de recursos en red y servicios distribuidos
- ❑ Gran diversidad de servicios

Tipos de servicios en red

Configuración y administración

- Gestión de equipos.
- Ej: DHCP.

Acceso remoto

- Se permite a los equipos remotos acceder a la red
- Ej: SSH

Gestión de archivos

- Transferencia, almacenamiento y gestión de archivos
- Ej: FTP.

Servicios de impresión

- Compartición de impresoras

Información

- Búsqueda y compartición de información
- Ej: WWW, compartición de video, IPTV

Comunicación

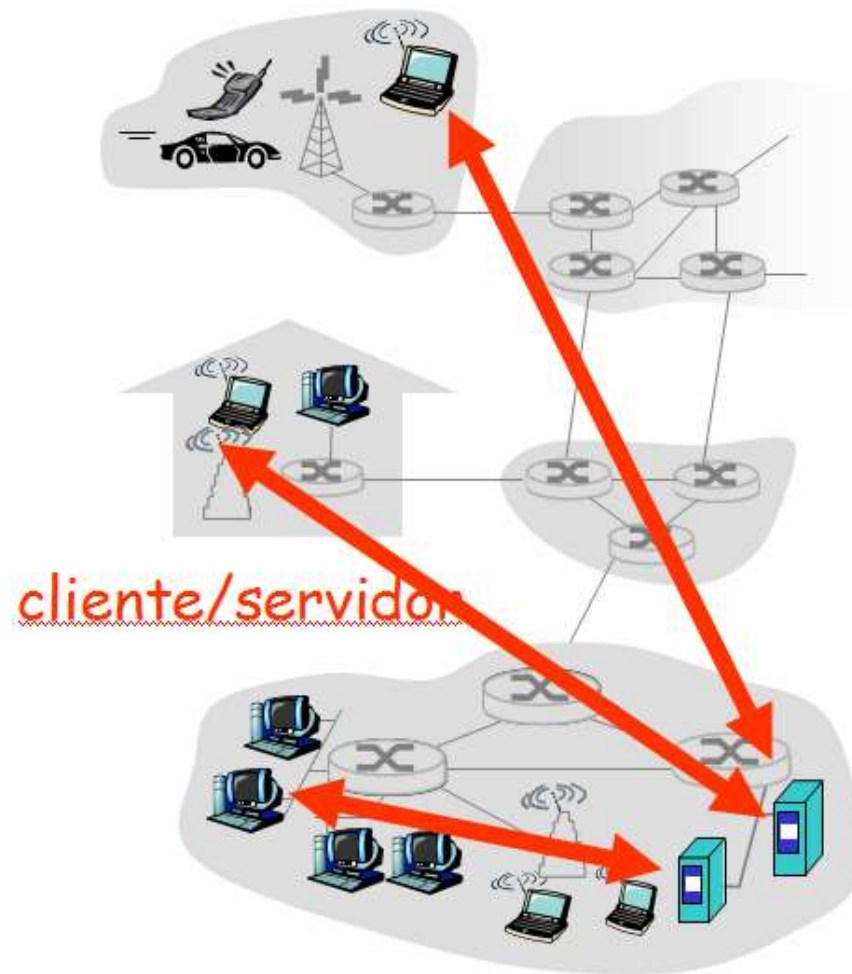
- Comunicación entre usuarios por medio de mensajes de texto, audio y/o video
- Ej: e-mail, chat, videoconferencia, telefonía IP, juegos online.

Arquitectura de los servicios en red

□ Paradigmas

- Cliente-servidor
- Peer-to-peer (P2P)
- Híbrido cliente-servidor y P2P

Arquitectura Cliente/Servidor



servidor:

- Siempre activo
- Dirección IP permanente
- Conjunto de servidores para un posible escalado

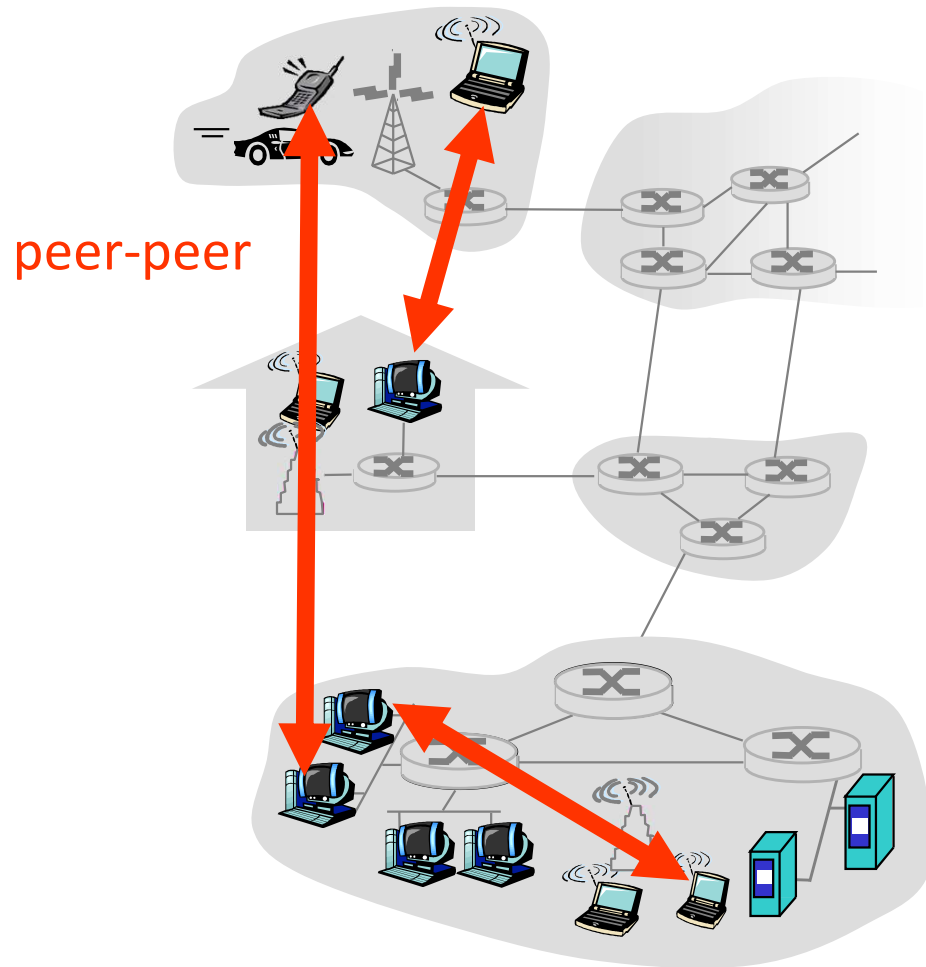
clientes:

- Se comunican con el servidor
- Pueden conectarse intermitentemente
- Pueden tener direcciones IPs dinámicas
- No se comunican directamente entre ellos

Arquitectura P2P

- ❑ Sin servidores que estén siempre activos
- ❑ Terminales arbitrarios pueden comunicarse entre sí.
- ❑ Los pares (peers) están intermitentemente conectados y pueden cambiar sus IPs

Sistemas muy escalables, pero difíciles de gestionar



Híbrido cliente-servidor y P2P

Arquitectura híbrida C/S – P2P

- Un servidor central sirve de enlace entre nodos de la red
- El servidor no ofrece los recursos, sino que solo permite la conexión entre nodos
- Los recursos se transmiten directamente entre clientes

Ejemplo: Skype

- Aplicación P2P de voz sobre IP (VoIP)
- Servidor centralizado: para encontrar la dirección remota de los usuarios
- Conexión cliente-cliente: directa (no a través del servidor)

Capítulo 2: Servicios en red

❑ 1.1 Introducción

❑ 1.2 Servicios de transferencia de archivos

- TFTP
- FTP

❑ 1.3 Servicios de correo electrónico

- SMTP
- POP3

❑ 1.4 Servicios de Nombres de Dominio (DNS)

Servicios de transferencia de archivos

- ❑ Transferencia de archivos entre hosts remotos
- ❑ Objetivos:
 - Compartición de archivos entre equipos remotos
 - Sistemas de archivos de cliente y servidor independientes
 - Transferencia de datos eficaz
- ❑ Dos protocolos principales
 - FTP (File Transfer Protocol): usa TCP -> fiable
 - RFC 959
 - TFTP (Trivial File Transfer Protocol): usa UDP -> más simple
 - RFC 1350

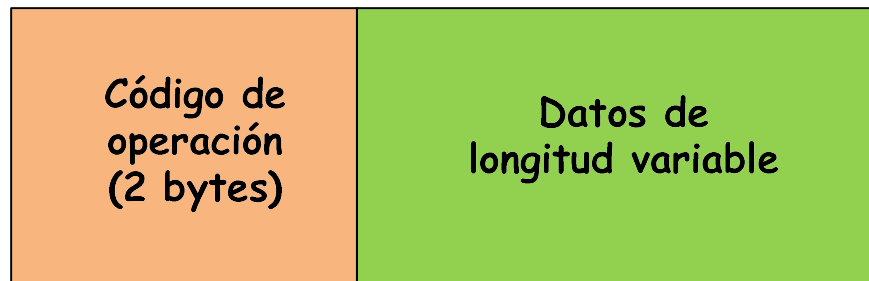
TFTP

❑ Trivial File Transfer Protocol

- Transferencia de ficheros
- Protocolo muy simple
- No fiable -> UDP (puerto 69)
- Sin carpetas; sin encriptación
- Para la transferencia de pequeños ficheros

TFTP

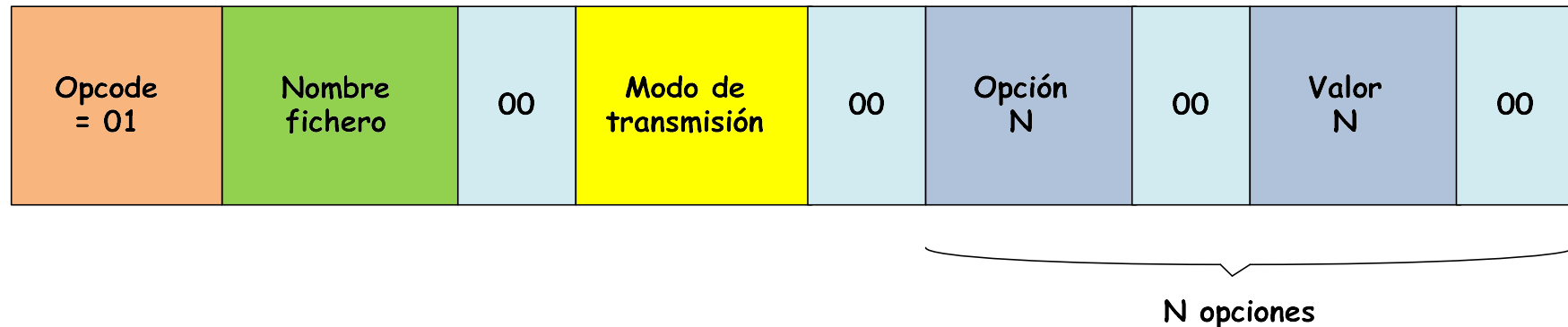
❑ Mensajes TFTP



- Código de operación (Opcode): tipo de mensaje
 - 01: RRQ (Read Request): Petición de lectura
 - 02: WRQ (Write Request): petición de escritura
 - 03: DATA
 - 04: ACK
 - 05: Mensaje de error
- Datos de longitud variable: dependen del opcode

TFTP

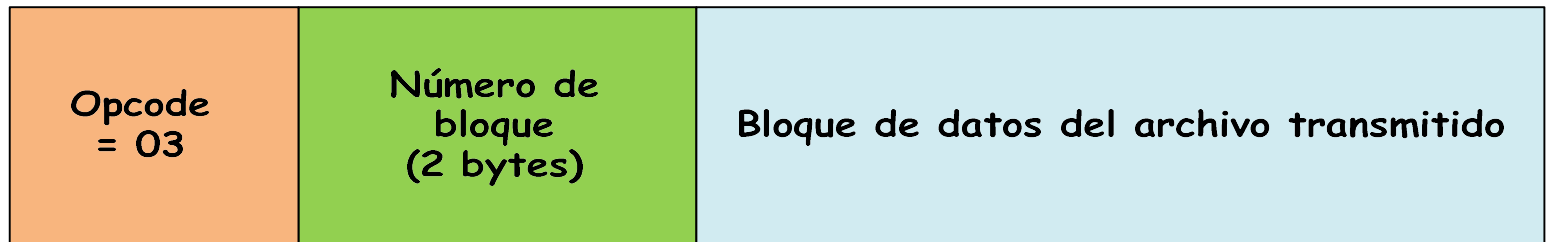
❑ Mensajes TFTP -> RRQ & WRQ



- RRQ es el primer mensaje que se envía al puerto 69 del servidor al bajar un archivo
- Después de RRQ -> DATA o Error
- Modo de transmisión: 'netascii' u 'octet' (archivos binarios)
- N opciones posibles con N valores (una para cada opción)
- El formato de los mensajes WRQ es el mismo que el de los RRQ -> pero opcode = 02
- Después de WRQ -> ACK (el servidor debe dar permiso) o Error

TFTP

❑ Mensajes TFTP -> DATA & ACK

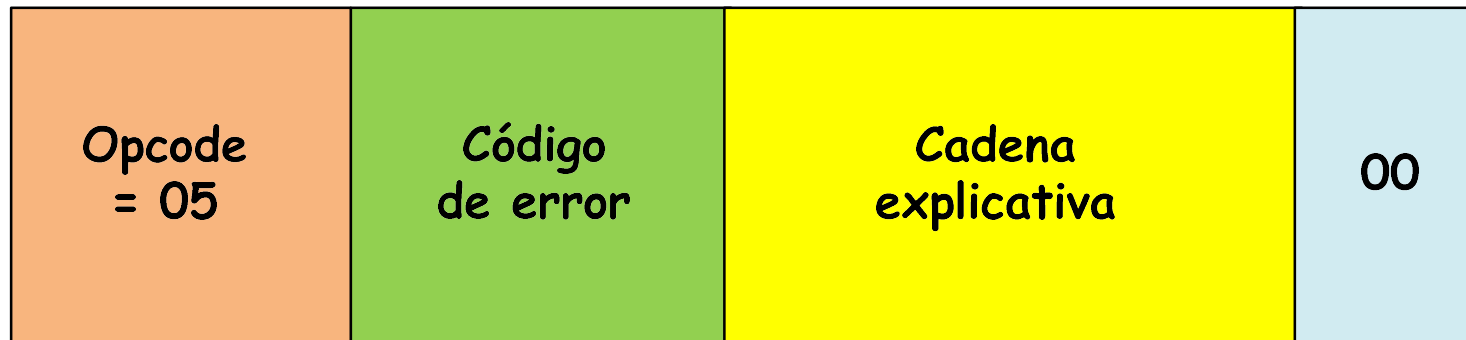


0-512 bytes

- Nº bloque -> 1-65535 (garantiza el orden de los datos -> UDP no puede)
- El último bloque se reconoce porque es < 512 bytes (¿qué ocurre si la long. total del archivo es múltiplo de 512 bytes?)
- Problema: archivos largos -> un mensaje perdido significa una retx. completa
- El formato de mensajes ACK es el mismo que el de DATA -> pero opcode = 04 y no hay bloques de datos

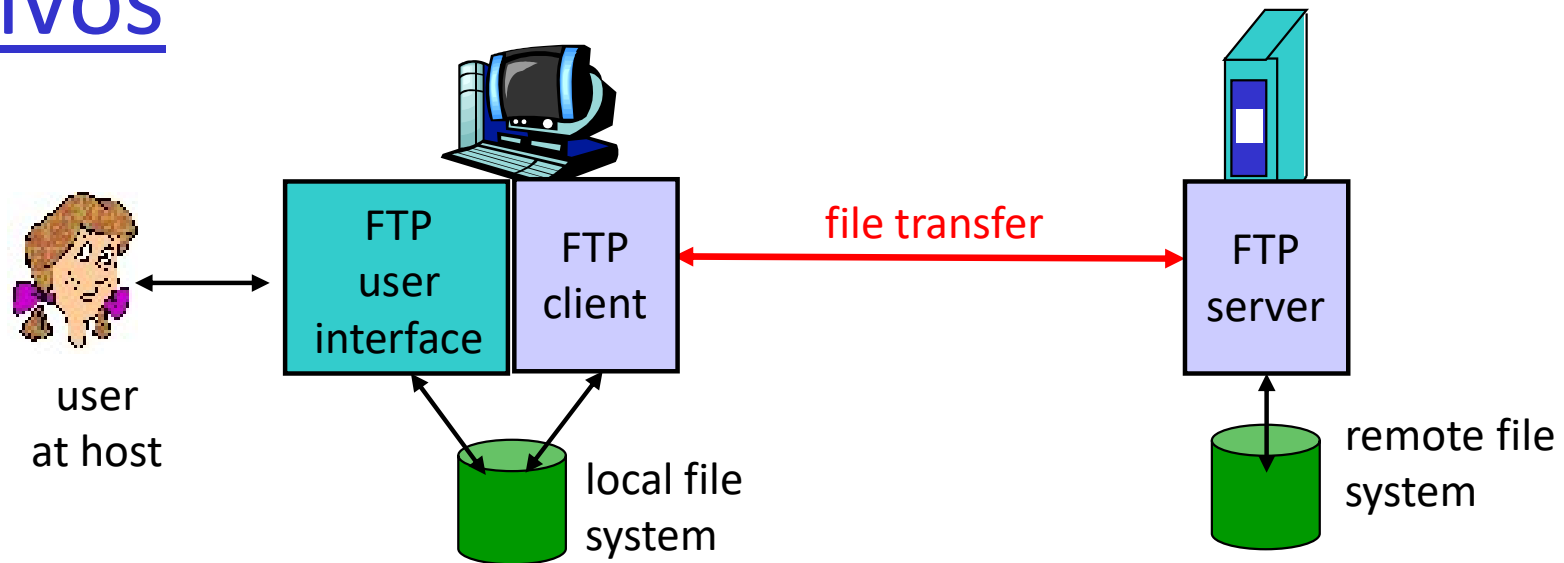
TFTP

❑ Mensajes TFTP -> Error



- Código de error: causa del error.
- Ejemplos
 - 0 -> No definido. Ver cadena explicativa
 - 1 -> File not found
 - 2 -> Access violation (el cliente no tiene permiso para la acción – lectura o escritura – realizada)
 - 3 -> Disk full
 - ...
 - 6 -> File already exists

FTP: protocolo de transferencia de archivos

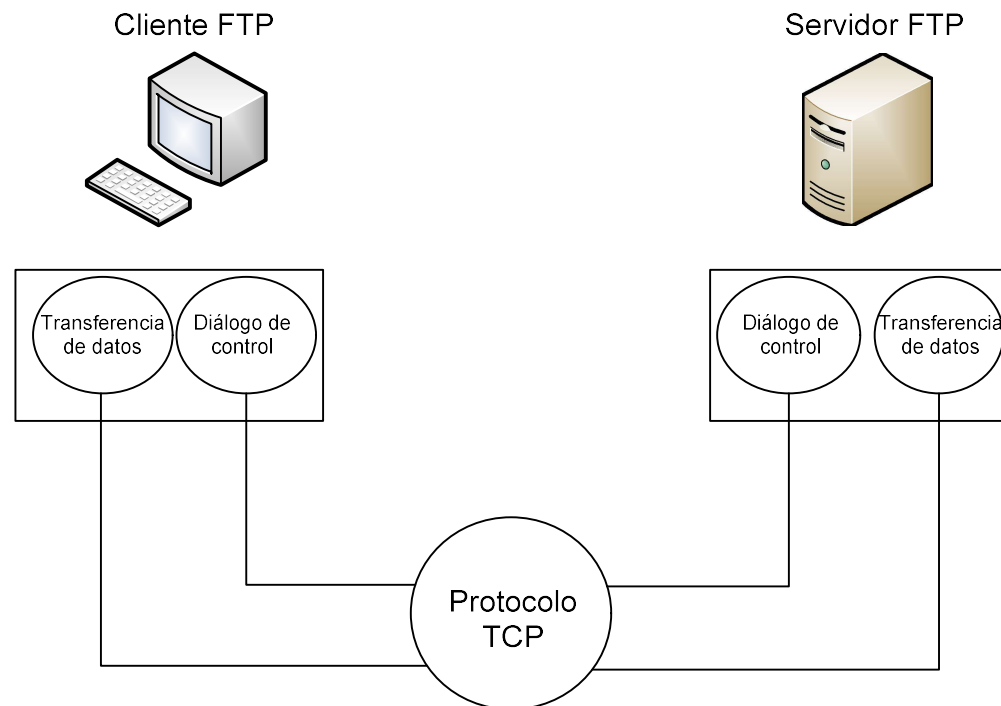


- ❑ Transferencia de ficheros de/hacia equipos remotos
- ❑ Modelo cliente/servidor
 - *cliente*: parte que inicia la transferencia (hacia/desde la parte remota)
 - *servidor*: equipo remoto
- ❑ ftp: RFC 959
- ❑ Usa TCP: puertos 20, 21 -> transferencia fiable

FTP

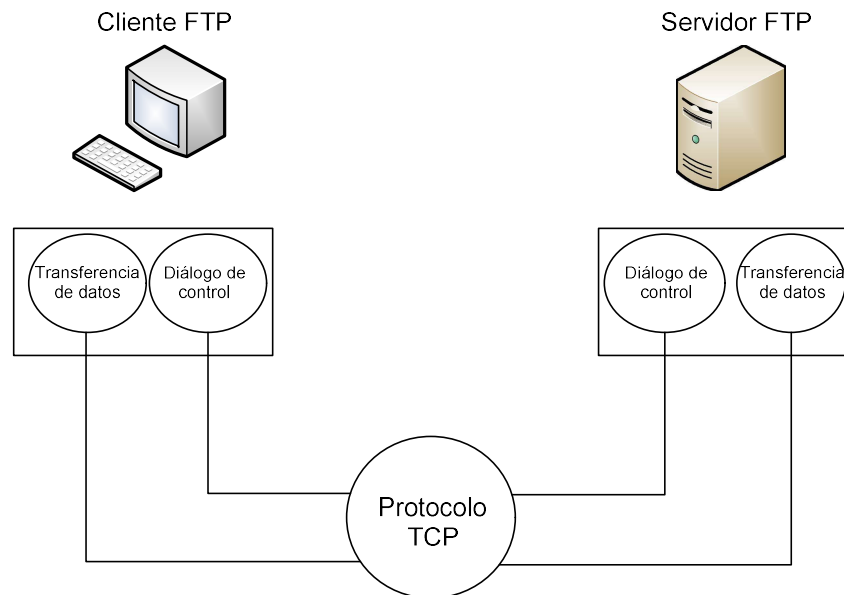
❑ Dos conexiones TCP

- **Control:** Inicia la comunicación con el servidor. Permite al usuario moverse por la estructura de directorios y bajar y subir archivos (puerto 21)
- **Datos:** conexión para transferir datos (puerto 20). Archivos y listado de directorios.



FTP: Modelo Cliente/Servidor

- ❑ El cliente FTP inicia la conexión (de control, al puerto 21 del servidor)
- ❑ Los parámetros de conexión se negocian en el establecimiento
 - Puerto de datos
 - Modo de conexión: activo/pasivo
 - Modo de transferencia: ASCII/binario



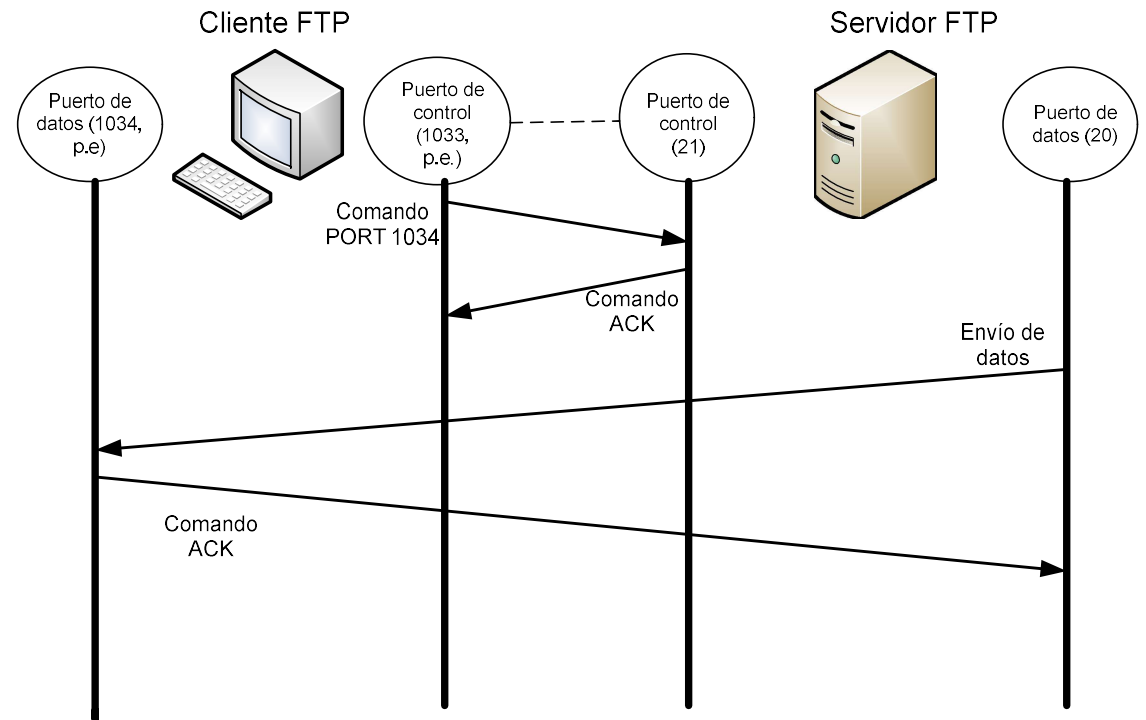
Modo de conexión activo

❑ Modo estándar

❑ 2 conexiones TCP

- Control: puerto aleatorio del cliente (>1024) al puerto 21 del servidor
- Datos: tras el ACK del servidor -> del puerto 20 del servidor al puerto del cliente (indicado en el primer comando de control)

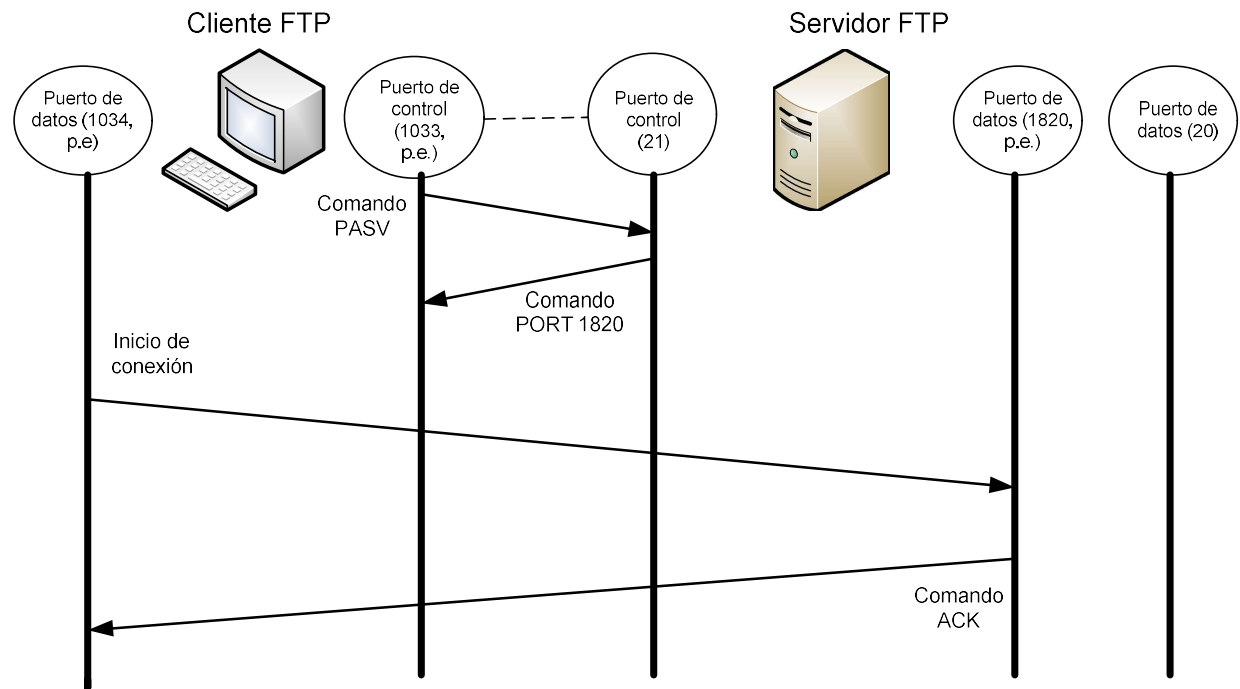
❑ El servidor inicia la conexión de datos



Modo de conexión pasivo

❑ 2 conexiones TCP

- Control: de un puerto aleatorio del cliente (>1024) al puerto 21 del servidor -> comando PASV. El servidor indica un puerto aleatorio para la conexión de datos (>1024)
- El cliente establece la conexión de datos (por ejemplo, para evitar firewalls)



FTP: Servidores

❑ Parámetros de configuración

- Puerto de control (por defecto: puerto 21)
- Máximo nº de conexiones al servidor y máximo nº de conexiones por IP
- Temporizador de conexión (timeout)
- Mensajes de bienvenida y despedida
- Números de puerto para el modo pasivo

❑ Usuarios y grupos

- Usuarios autenticados: con login y passwd -> registrados en el servidor
- Usuarios anónimos
- Grupos: comparten las mismas propiedades en el servidor FTP

FTP: Servidores

❑ Permisos

- Read, write, execution (rwx)
- Permisos para el propietario, grupos y resto de usuarios

❑ Límite de BW

- El servidor puede limitar la velocidad de transferencia a los usuarios

❑ Logs

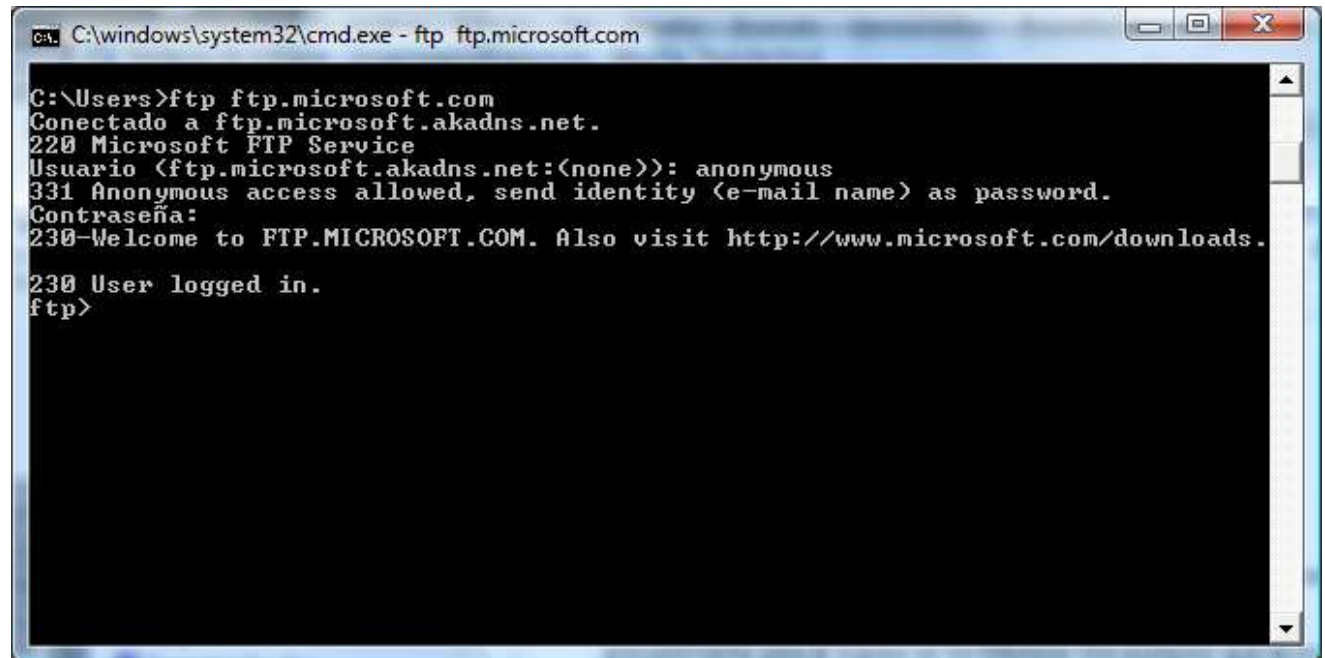
- Registran datos o cualquier otra info sobre conexiones de los usuarios y errores

FTP: Clientes

❑ ftp <ip_addr>

❑ Comandos

- cd
- get
- put
- mkdir
- exit
- ...
- No hay que confundir los **comandos FTP** escritos por el cliente en la consola con los **comandos de control FTP**



```
C:\windows\system32\cmd.exe - ftp ftp.microsoft.com

C:\Users>ftp ftp.microsoft.com
Conectado a ftp.microsoft.akadns.net.
220 Microsoft FTP Service
Usuario <ftp.microsoft.akadns.net:(none)>: anonymous
331 Anonymous access allowed, send identity (e-mail name) as password.
Contraseña:
230-Welcome to FTP.MICROSOFT.COM. Also visit http://www.microsoft.com/downloads.
230 User logged in.
ftp>
```

FTP: comandos, respuestas

Ejemplos de comandos de control:

Se envían como texto ASCII por el canal de control

- ❑ **USER *username***
- ❑ **PASS *password***
- ❑ **LIST** devuelve la lista de archivos del directorio actual.
- ❑ **RETR filename** descarga (get) el archivo.
- ❑ **STOR filename** sube (put) el archivo al host remoto.
- ❑ **PORT IP, puerto** abre un puerto del host para la conexión de datos

Ejemplos de códigos de respuesta

Código de estado y frase (como en HTTP)

- ❑ **331 Username OK, password required**
- ❑ **125 data connection already open; transfer starting**
- ❑ **425 Can't open data connection**
- ❑ **452 Error writing file**

Capítulo 2: Servicios en red

- ❑ 1.1 Introducción
- ❑ 1.2 Servicios de transferencia de archivos
 - TFTP
 - FTP
- ❑ 1.3 Servicios de correo electrónico
 - SMTP
 - POP3
- ❑ 1.4 Servicios de Nombres de Dominio (DNS)

Servicios de correo electrónico

Características principales:

- ❑ Uno de los servicios más importantes de Internet
- ❑ Permite que dos usuarios intercambien “cartas” de manera fácil, rápida y barata.
- ❑ Multitud de destinatarios
- ❑ Esquema cliente-servidor
- ❑ Tipos de aplicaciones clientes:
 - Interfaz gráfica (Microsoft Outlook, Mozilla Thunderbird, Apple Mail)
 - Texto (pine, elm, mail)
 - Web (Gmail, Hotmail, SquirrelMail)

Servicios de correo electrónico

Conceptos relacionados:

- ❑ Cuenta de correo

- Asociado a un nombre de usuario y contraseña
usuario@dominio

- ❑ Buzón de correo

- ❑ Alias de correo

- ❑ Lista de correo

Servicios de correo electrónico

Estándares:

- ❑ SMTP (Simple Mail Transfer Protocol)
- ❑ IMF (Internet Mail Format)
- ❑ MIME (Multipurpose Internet Mail Extensions)
- ❑ POP (Post Office Protocol)
- ❑ IMAP (Internet Message Access Protocol)

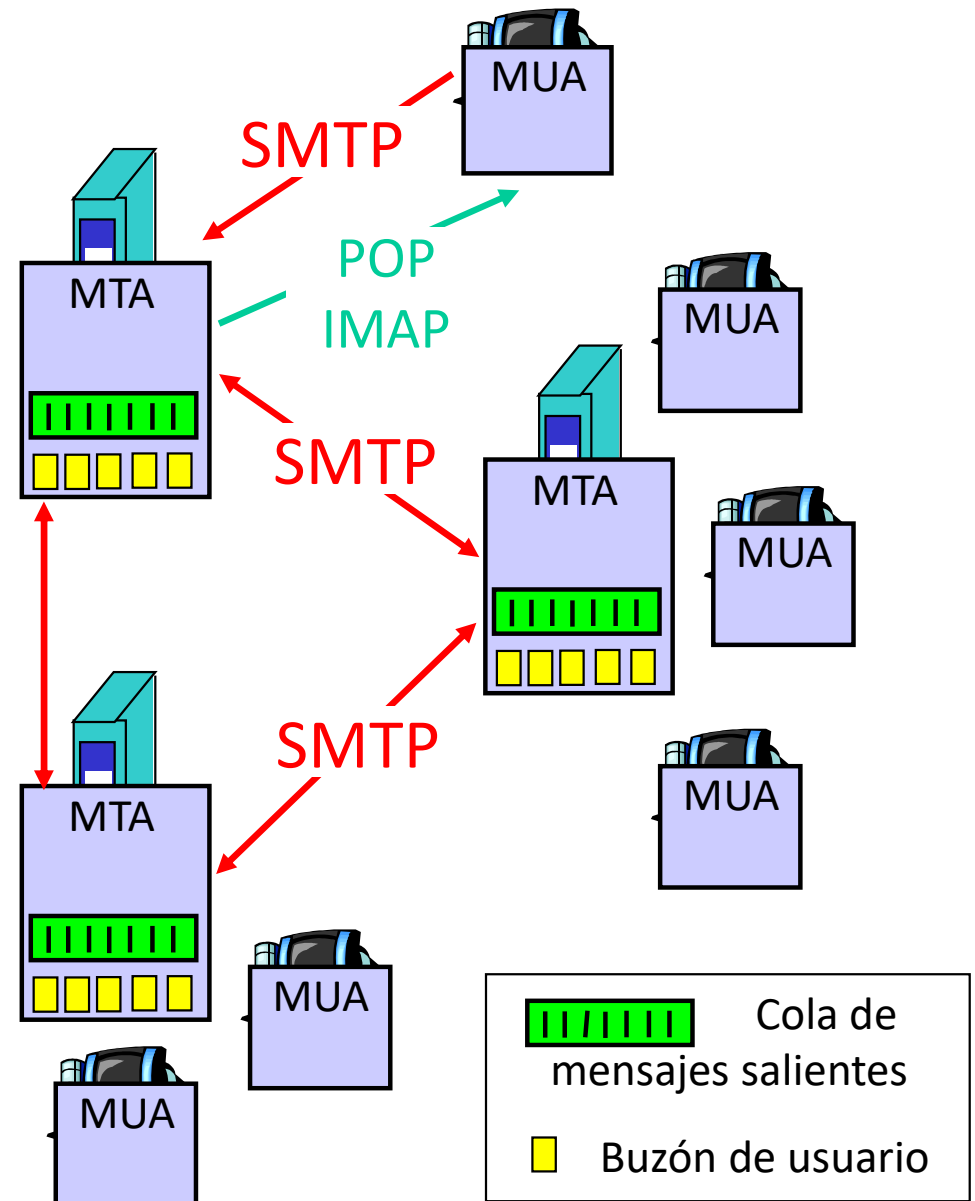
Servicios de correo electrónico

Componentes:

- ❑ Mail User Agent (MUA)
- ❑ Mail Transfer Agent (MTA)
- ❑ Mail Delivery Agent (MDA)

Agente de usuario (MUA)

- ❑ Cliente de correo
- ❑ Componer, editar, leer mensajes de correo
- ❑ Emplean dos servidores de correo:
 - Servidor de correo saliente (SMTP)
 - Servidor de correo entrante (POP o IMAP)



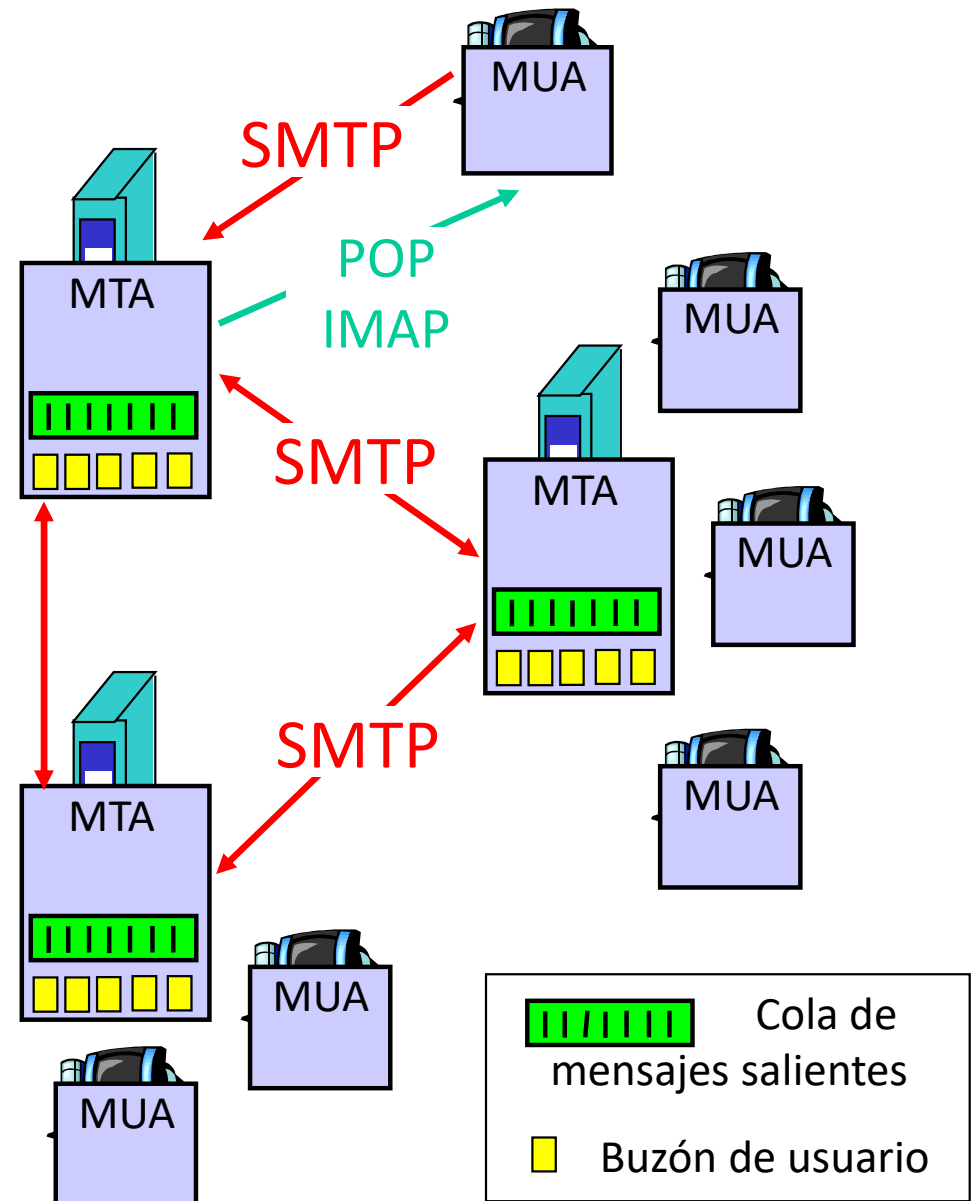
Servicios de correo electrónico

Agente de transferencia (MTA)

- ❑ Servidor de correo
- ❑ Almacena los correos de los remitentes para su envío (cola saliente)
- ❑ Almacena los correos entrantes de sus usuarios

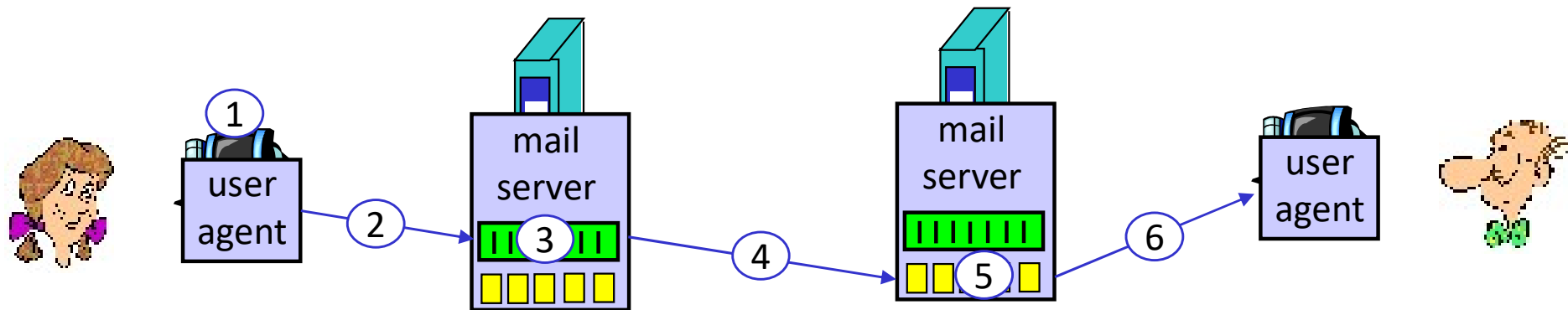
Agente de envío (MDA)

- ❑ Encargado de copiar los mensajes entrantes al buzón de correo del usuario
- ❑ Habitualmente integrado en MTA



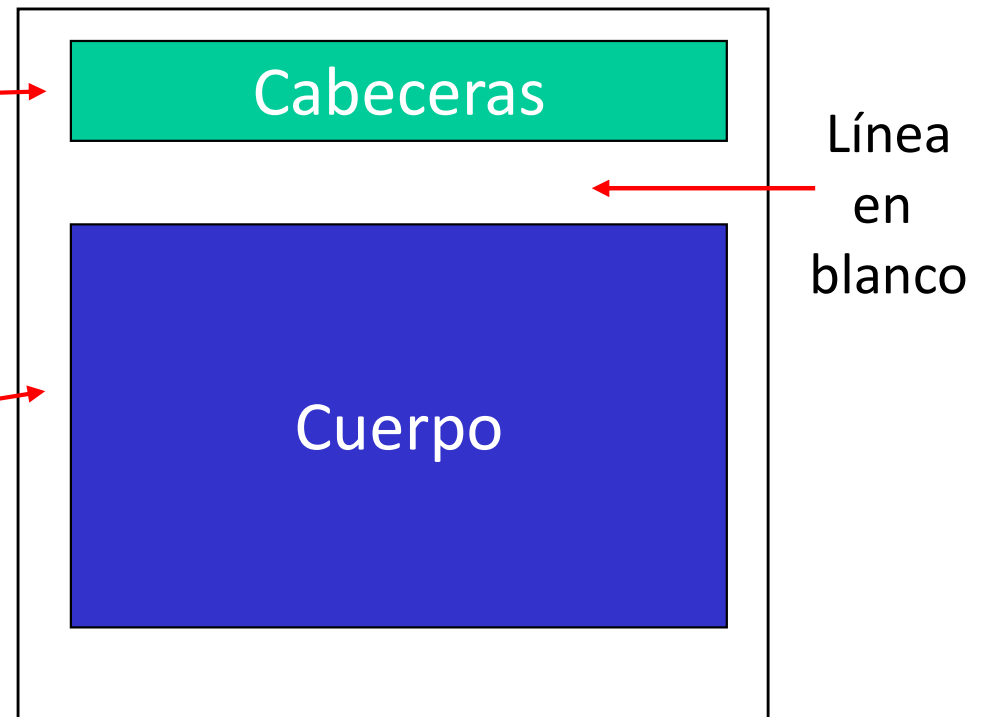
Escenario: Alice envía mensaje a Bob

- 1) Alice usa su cliente de correo (MUA) para componer el mensaje y "to" bob@dominioBob.es
- 2) El MUA de Alice envía el mensaje a su servidor de correo; El mensaje se coloca en la cola de mensajes salientes
- 3) El Cliente SMTP del servidor de correo de Alice abre una conexión TCP con el servidor de correo de Bob
- 4) El cliente SMTP envía el mensaje de Alice sobre la conexión TCP
- 5) El servidor de correo de Bob coloca el mensaje en el buzón de correo de Bob
- 6) Bob emplea su cliente de correo para acceder a los mensajes entrantes (POP o IMAP) y leerlos



Formato de los mensajes

- ❑ IMF (RFC 5322)
- ❑ Cabeceras
 - To:
 - From:
 - Subject:
 - Date:
- ❑ Cuerpo
 - Mensajes de texto simple (no ASCII extendido) de hasta 998 caracteres (sin CRLF)



Formato de los mensajes

Extensiones MIME:

❑ Añaden funcionalidad

- Ficheros adjuntos
- ASCII extendido

❑ Nuevas cabeceras

- Mime-Version:
- Content-Type:
 - ❖ Defecto -> text/plain
 - ❖ Adjuntos -> Multipart
- Content-Description:
- Content-Transfer-Encoding:

❑ Tipos de codificación

- 7 bits
- 8 bits y binary
- quoted-printable y base64.

Ejemplo quoted-printable

F3 = ó y F1 = ñ

Transmisión de ñ

Transmisi=F3n de =F1

SMTP [RFC 5321]

Características:

- ❑ Funcionamiento sencillo: cliente – servidor
- ❑ Usado en comunicación entre MUA → MTA y MTA → MTA
- ❑ Usa conexión **TCP** con puerto 25
- ❑ Tres fases
 - handshaking (saludo)
 - transferencia del mensaje (pueden ser varios)
 - cierre de conexión
- ❑ Los mensajes se codifican en ASCII de 7 bits

SMTP [RFC 5321]

Características:

□ comando/respuesta

respuesta: texto libre y código de estado (3 cifras):

- Primera cifra indica el éxito/fracaso del comando
 - ❖ 4xx -> Error temporal
 - ❖ 5xx -> Error permanente

comandos: Texto ASCII

- **HELO**: saludo tras aceptar conexión
- **MAIL FROM**: identifica remitente
- **RCPT TO**: indica destinatario
- **DATA**: inicio del mensaje
 - ❖ Fin del mensaje línea con ‘.’
- **QUIT**: Cierra sesión SMTP

- No hay que confundir las **cabeceras de correo** (from, to...) con los **comandos de control SMTP** (MAIL FROM, RCPT TO,...)

Ejemplo de SMTP

S: 220 hamburger.edu
C: HELO crepes.fr
S: 250 Hello crepes.fr, pleased to meet you
C: MAIL FROM: <alice@crepes.fr>
S: 250 alice@crepes.fr... Sender ok
C: RCPT TO: <bob@hamburger.edu>
S: 250 bob@hamburger.edu ... Recipient ok
C: DATA
S: 354 Enter mail, end with "." on a line by itself
C: Do you like ketchup?
C: How about pickles?
C: .
S: 250 Message accepted for delivery
C: QUIT
S: 221 hamburger.edu closing connection

□ Nota: La comunicación representada es un diálogo de aplicación bastante simplificado. Lógicamente, es necesaria una conexión TCP, así como todas las T_PDUs de control pertinentes.

POP [RFC 1939]

Características:

- ❑ Muy simple
- ❑ Permite acceder a los mensajes del buzón de correos entrante
- ❑ El comportamiento por defecto es borrar los mensajes accedidos, aunque permite guardarlos
- ❑ Usa conexión **TCP** con puerto 110
- ❑ Requiere autenticación de usuario
- ❑ Tres fases
 - autorización
 - transacción
 - actualización

POP [RFC 1939]

Fase de autorización

- ❑ comandos cliente:
 - **user:** declara el nombre de la cuenta del usuario
 - **pass:** contraseña
- ❑ respuestas del servidor
 - **+OK**
 - **-ERR**

Fase de transacción

- ❑ **list:** muestra los identificadores de los mensajes
- ❑ **retr:** descarga el mensaje indicado por su identificador
- ❑ **dele:** borra el mensaje indicado
- ❑ **quit**

S: +OK POP3 server ready
C: user bob
S: +OK
C: pass hungry
S: +OK user successfully logged on

C: list
S: 1 498
S: 2 912
S: .
C: retr 1
S: <message 1 contents>
S: .
C: dele 1
C: retr 2
S: <message 1 contents>
S: .
C: dele 2
C: quit
S: +OK POP3 server signing off

IMAP [RFC 3501]

Características:

- ❑ Más complejo que POP
- ❑ Permite acceder a los mensajes del buzón de correos entrante
- ❑ Permite organizar los mensajes en carpetas en el servidor
- ❑ Al recibir un nuevo correo, se coloca en la carpeta INBOX del buzón del usuario
- ❑ Posibilita el acceso a partes componentes de un mensaje
- ❑ Conserva información del estado entre sesiones IMAP

Acceso web

Características:

- ❑ Se utiliza un navegador en lugar de un cliente de correo
- ❑ MUA está integrado en una página web
- ❑ El equipo del usuario emplea el protocolo HTTP para comunicarse con el servidor web
- ❑ El MUA integrado en la página web se comunica con el servidor de correo mediante SMTP
- ❑ El servidor web generalmente emplea IMAP para acceder a los mensajes entrantes del servidor de correo

Problemas

Principales problemas:

- ❑ los mensajes se transmiten en claro
 - Emplear mecanismos de seguridad (PGP, PEM, s/MIME)
- ❑ Usos indebidos
 - SPAM

SPAM

- ❑ Contacto con muchos a bajo coste
- ❑ Correo masivo no solicitado
- ❑ Tipos
 - Comercial
 - Nigeriano
 - Phishing
 - Otros
- ❑ Origen
 - equipo de una persona
 - servidores de correo mal configurados
 - servidores proxy mal configurados

SPAM

- ❑ Cómo obtienen direcciones destinatarios:
 - adivinar
 - página web
 - ordenador infectado
- ❑ Falsifican las cabeceras de correo (FROM)
- ❑ Cómo evitarlos
 - impedir/dificultar obtención de direcciones de correo
 - identificarlos eficientemente
- ❑ Medidas
 - no publicar nuestra dirección de correo
 - publicar nuestra dirección de correo de forma protegida
 - usar direcciones alternativas
 - vigilar la seguridad de nuestro ordenador

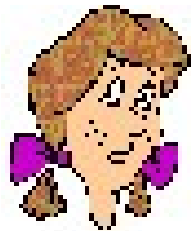
Capítulo 2: Servicios en red

- ❑ 1.1 Introducción
- ❑ 1.2 Servicios de transferencia de archivos
 - TFTP
 - FTP
- ❑ 1.3 Servicios de correo electrónico
 - SMTP
 - POP3
- ❑ 1.4 Servicios de Nombres de Dominio (DNS)

DNS: Sistema de Nombres de Dominio

Planteamiento:

- ❑ Desde el punto de vista del usuario
 - Identifica el “elemento” poseedor del recurso mediante dirección (www.dte.us.es)



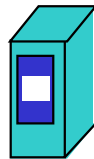
DNS: Sistema de Nombres de Dominio

Equipos de internet, routers:

- ❑ Dirección IP (32 bits) – usados para direccionar datagrama
- ❑ “nombre”, ej: www.google.es - usado por los seres humanos

¿Cómo se genera el nombre?

Elemento poseedor
de recurso



150.214.141.196

www.dte.us.es

DNS: Sistema de Nombres de Dominio

Sistemas de nombres:

☐ Planos

- No jerárquico
- No informa de localización
- Ej: DNI

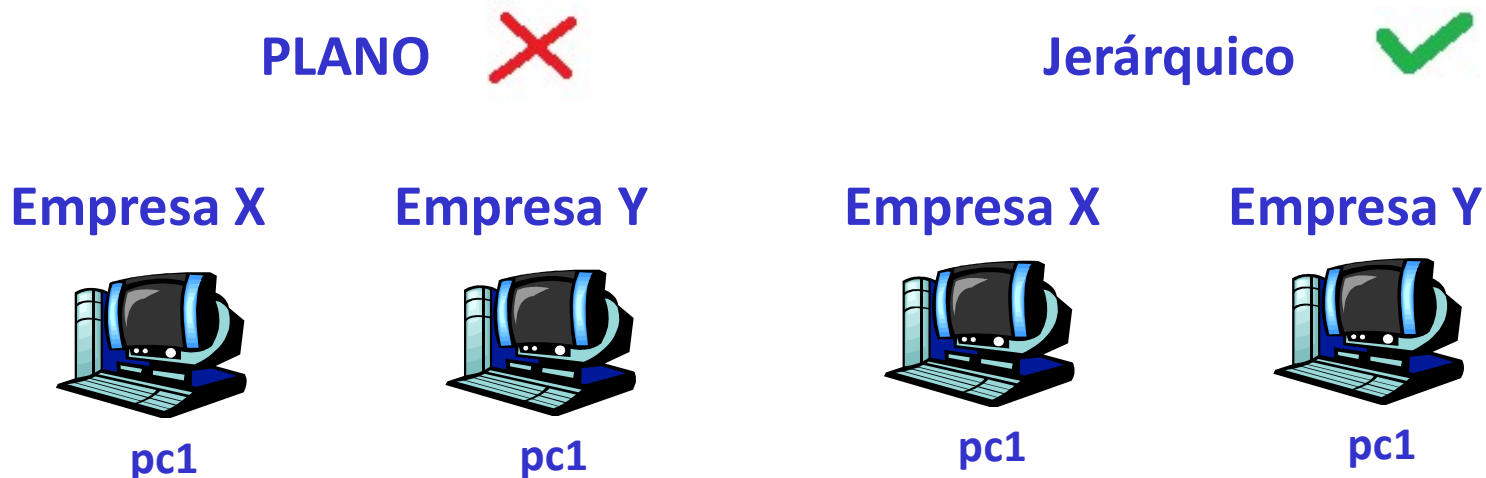
☐ Jerárquico

- Con estructura
- Informan de localización
- Ej: Dirección postal

DNS: Sistema de Nombres de Dominio

Sistemas de nombres:

- ❑ Planos sencillos -> administración centralizada
- ❑ Jerárquico -> Facilita administración (distribuida) - DNS



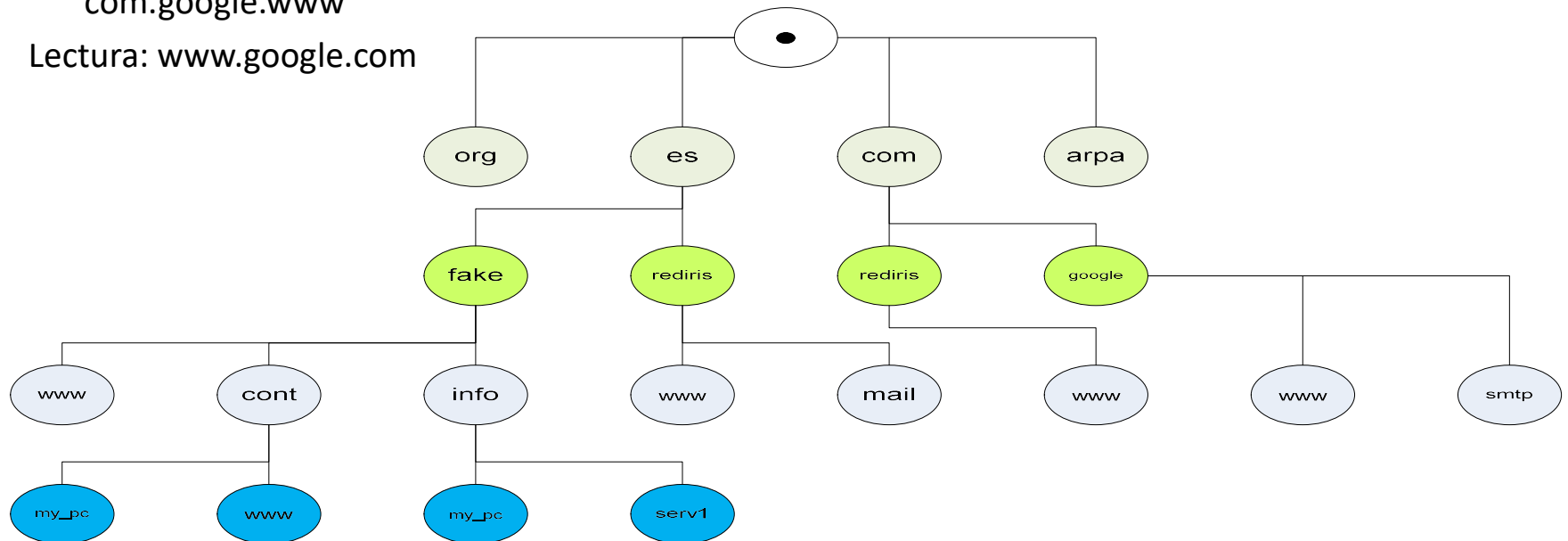
DNS: Sistema de Nombres de Dominio

Espacio de nombres:

- ❑ Estructura de árbol invertido
- ❑ Cada elemento etiquetado con nombre (máximo 63 caracteres)
- ❑ Comienzo de árbol -> raíz (etiqueta vacía)
- ❑ Profundidad variable (máximo 127 niveles)
- ❑ Similar estructura de directorios de SS.OO.
- ❑ Recorrido para formar nombre (raíz -> hoja)

com.google.www

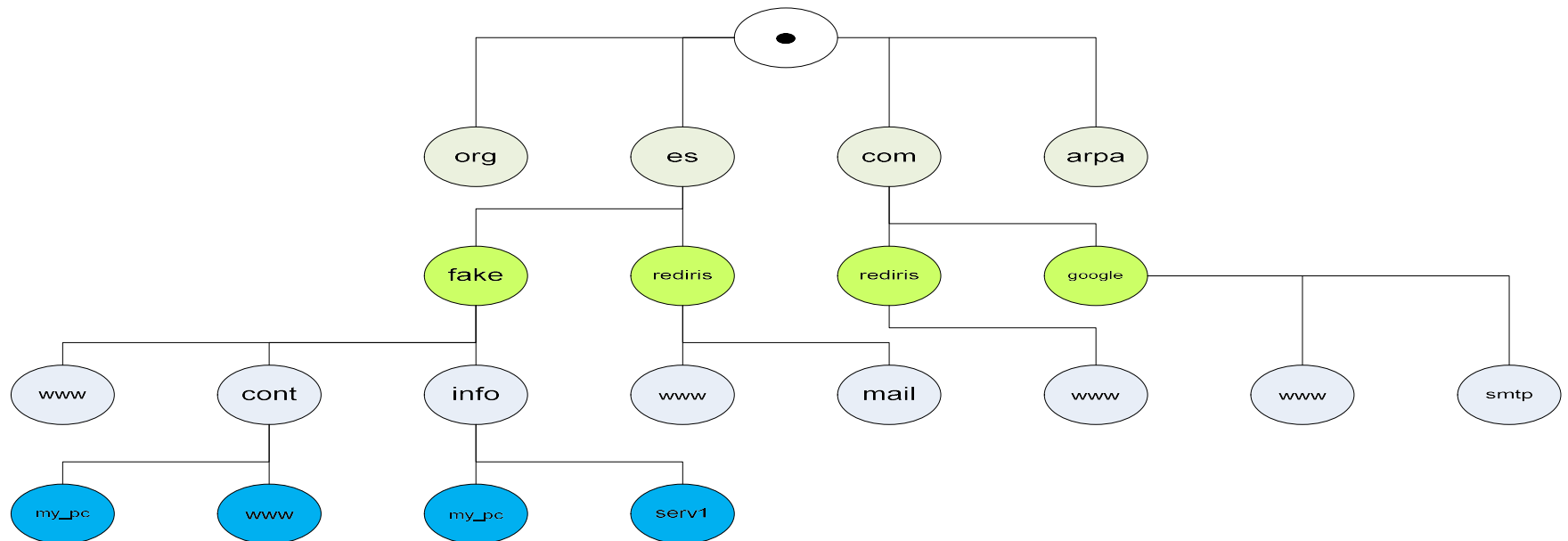
- ❑ Lectura: www.google.com



DNS: Sistema de Nombres de Dominio

Espacio de nombres:

- ❑ Importante
 - ❑ Raíz no etiquetada
 - ❑ Cada dominio representa un subárbol
 - ❑ Dominios organizados en niveles
 - ❑ Dominios de primer nivel (TLD)
 - ❑ Puede asignarse la misma etiqueta a dos equipos siempre que no sean hermanos



DNS: Sistema de Nombres de Dominio

Espacio de nombres:

my_pc.cont.fake.es.



DNS: Sistema de Nombres de Dominio

Sistema de Nombres de Dominio:

- ❑ *Base de datos distribuida* implementada en una jerarquía de muchos *servidores de nombres*
- ❑ *Protocolo de la capa de aplicación:* permite a los equipos consultar la base de datos distribuida para obtener la dirección IP asociada a un nombre
- ❑ DNS utiliza habitualmente los servicios de UDP (puerto 53)

Servicios DNS

- ❑ Traducción entre el nombre del equipo y la dirección IP
- ❑ Alias de los hosts
 - Traducción entre nombres canónicos y alias
- ❑ Alias de servidores de correo
- ❑ Distribución de la carga
 - Servidores Web replicados: conjunto de IPs para un solo nombre canónico

DNS: Sistema de Nombres de Dominio

Fundamentos básicos

1. La aplicación necesita saber la IP remota asociada a un nombre
2. La aplicación pide la IP al cliente DNS
3. El cliente DNS manda una petición a la red
4. El cliente DNS recibe una respuesta que incluye la IP
5. El cliente DNS da la IP a la aplicación

Por qué no centralizar DNS?

- Un único punto de fallo
- Volumen de tráfico
- Base de datos centralizada distante
- Mantenimiento

El enfoque centralizado no sería escalable

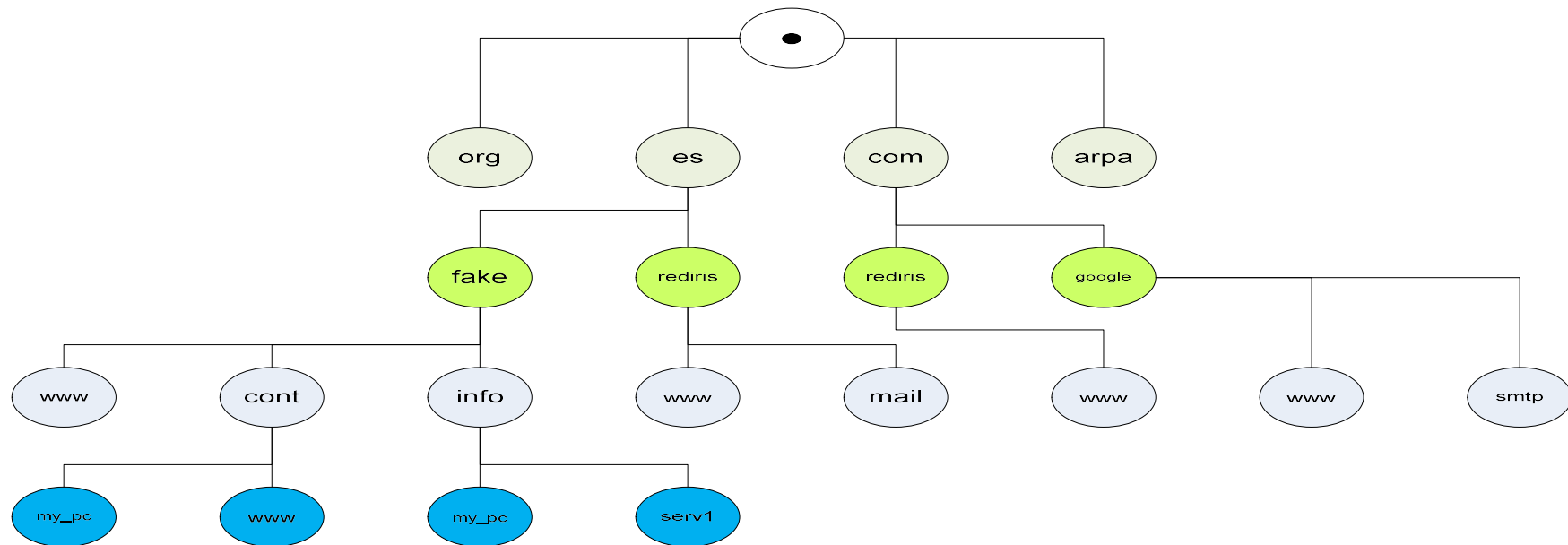
Servidores DNS locales

- ❑ No pertenecen estrictamente a la jerarquía
- ❑ cada ISP (ISP residencial, empresa, universidad) tiene uno.
 - También llamados “default name server”
- ❑ Cuando los hosts hacen una petición DNS, la envían a estos servidores locales
 - El servidor local actúa como proxy y lleva la petición hacia la jerarquía
- ❑ Cualquier servidor DNS de la jerarquía puede hacer de servidor DNS local

Base de datos distribuida y jerárquica

- ❑ Gran número de servidores DNS organizados jerárquicamente y distribuidos por todo el mundo
- ❑ La base de datos está distribuida por estos servidores
- ❑ Tres tipos de servidores:
 - Servidores raíz
 - Servidores de dominio de nivel superior (Top-Level Domain, TLD)
 - Servidores autoritativos

Base de datos distribuida y jerárquica



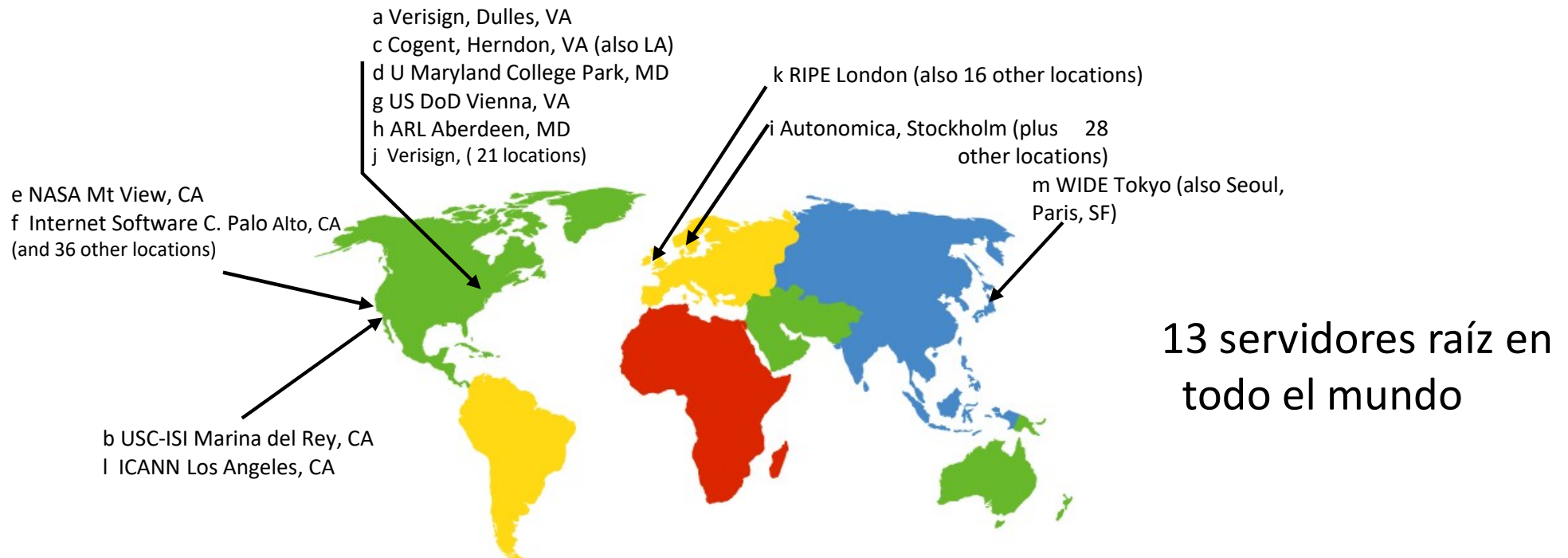
Ej: el cliente quiere la IP de www.google.com; 1ª aprox:

- ❑ El cliente contacta con un servidor raíz para encontrar el servidor TLD .com
- ❑ El cliente contacta con el servidor DNS .com correspondiente para devolver la dirección de un servidor DNS autoritativo para google.com
- ❑ El cliente busca la IP en el servidor autoritativo de www.google.com

DNS: Servidores raíz

❑ Servidores raíz:

- contactan con servidores de nivel jerárquico inferior si no son capaces de mapear el nombre pedido
- reciben el mapeo
- devuelven el mapeo al servidor local.



Servidores TLD y Autoritativos

❑ Servidores de dominio de nivel superior (Top-level domain, TLD) :

- responsables de .com, .org, .net, .edu, etc, y todos los dominios de nivel superior nacionales (.uk, .fr, .es, .jp)
- Network Solutions mantiene los servidores TLD .com
- Educause hace lo propio para los .edu
- Tipos
 - Genéricos (gTLD)
 - ❖ 3 o + caracteres
 - ❖ Patrocinados
 - ❖ No patrocinados

Servidores TLD y Autoritativos

❑ Servidores de dominio de nivel superior (Top-level domain, TLD) :

- Tipos
 - Geográficos
 - ❖ 2 caracteres
 - ❖ Representa países (gestionados por entidades de los mismos)
 - ❖ ICANN -> IANA
 - .arpa
 - Reservados
 - ❖ .test -> pruebas DNS.
 - ❖ .localhost -> loopback
 - Desde hace unos años ICANN es más permisivo con los nombres de dominio y estos han aumentado de forma importante

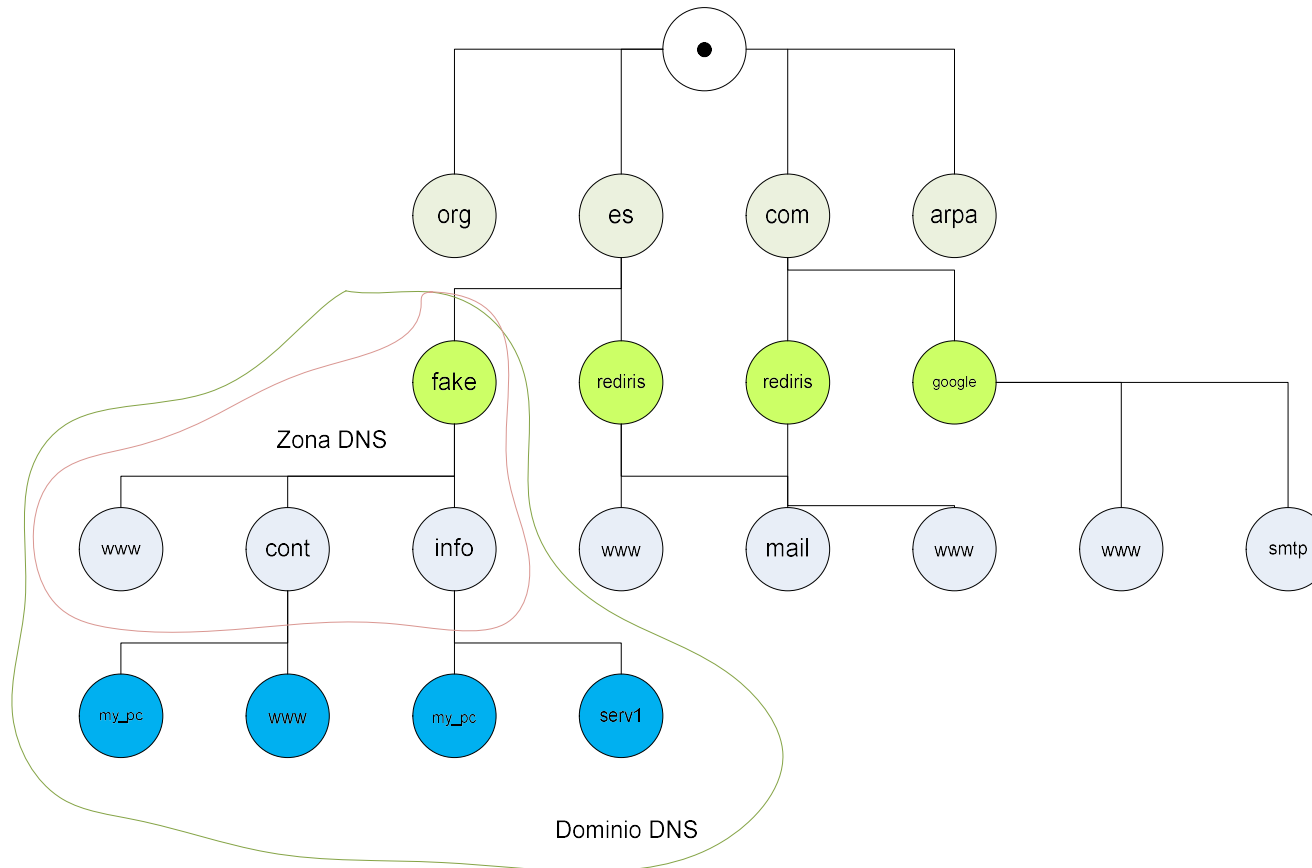
Servidores TLD y Autoritativos

❑ Servidores DNS Autoritativos:

- Son los servidores DNS que contienen los nombres de los recursos de empresas y organizaciones.
- Organizaciones con servidores públicos (web o correo, por ej.) -> registros DNS públicos para poder resolver los nombres de dichos servidores
- Administración por la propia organización o contratación de algún proveedor de servicios.
- Hasta hace no mucho, era habitual que grandes empresas e instituciones gestionaran y mantuvieran sus propios servidores autoritativos, pero la tendencia actual conduce a la contratación de empresas especializadas

Zonas DNS vs. Dominios DNS

- ❑ Dominio DNS: incluyen todas las máquinas y subdominios pertenecientes al dominio en cuestión.
- ❑ Zona DNS: sólo incluyen las máquinas del dominio

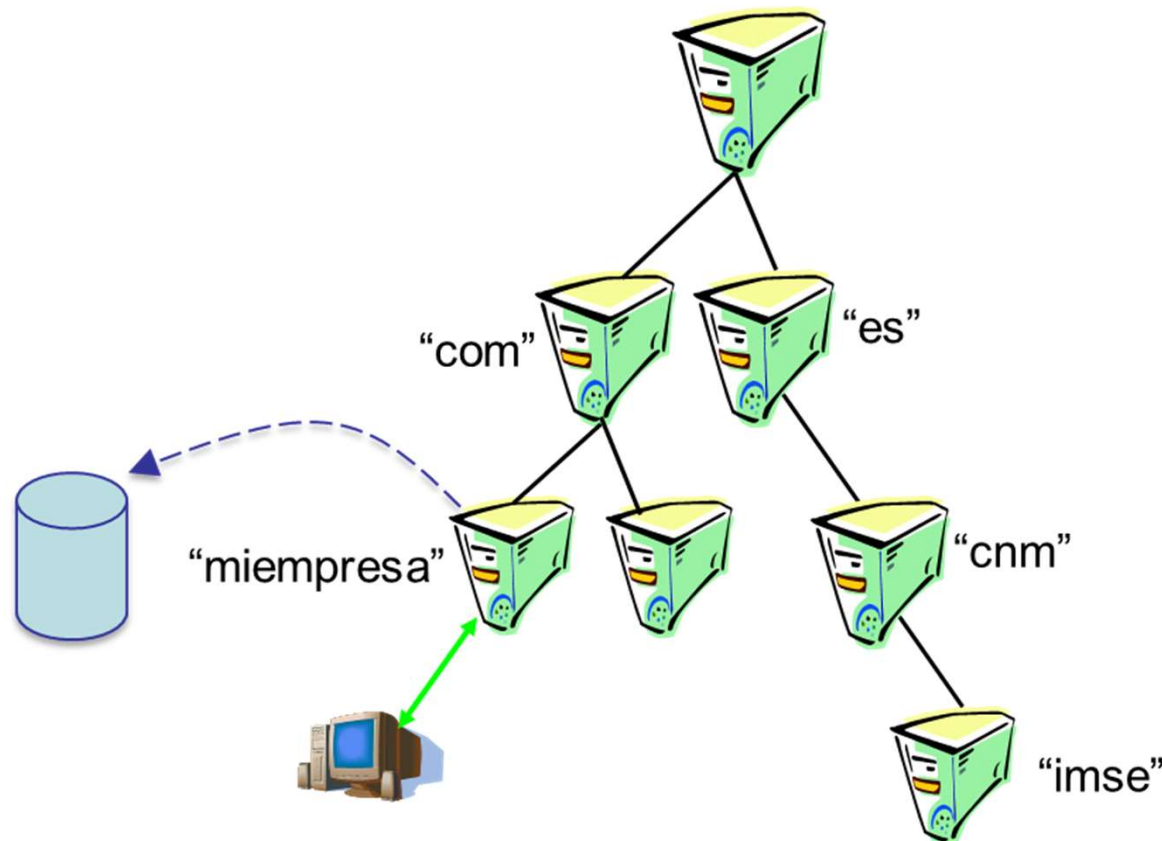


DNS: caché y actualizaciones

- ❑ Una vez que un servidor de nombres aprende el mapeo, lo introduce en una **caché**
 - Transcurrido un tiempo, las entradas de la caché se borran
 - Los servidores TLD están habitualmente en la caché de los servidores locales
 - Esto permite saltarse a los servidores raíz
- ❑ Los mecanismos de actualización/notificación están bajo la responsabilidad del IETF
 - RFC 2136
 - <http://www.ietf.org/html.charters/dnsind-charter.html>

Resolución de nombres DNS

- Un servidor DNS intentará responder con lo que tenga en sus mapas de direcciones propios y su caché.
- Si no sabe como llegar a alguna URL, debe buscar su IP.



Resolución de nombres DNS

❑ Tipos de consultas DNS

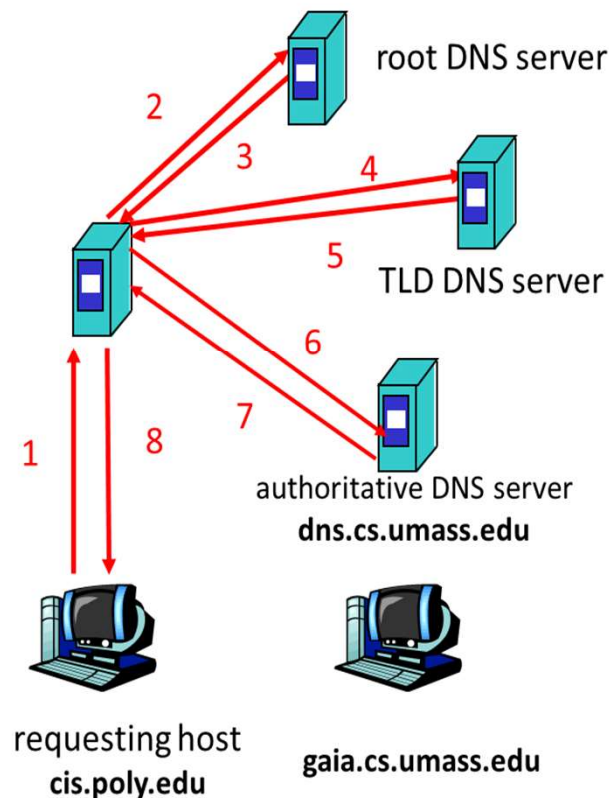
Consulta iterativa:

- Los servidores DNS a los que se pregunta devuelven el nombre de otro servidor DNS al que preguntar
- “No puedo resolver ese nombre, pregunte a este servidor”

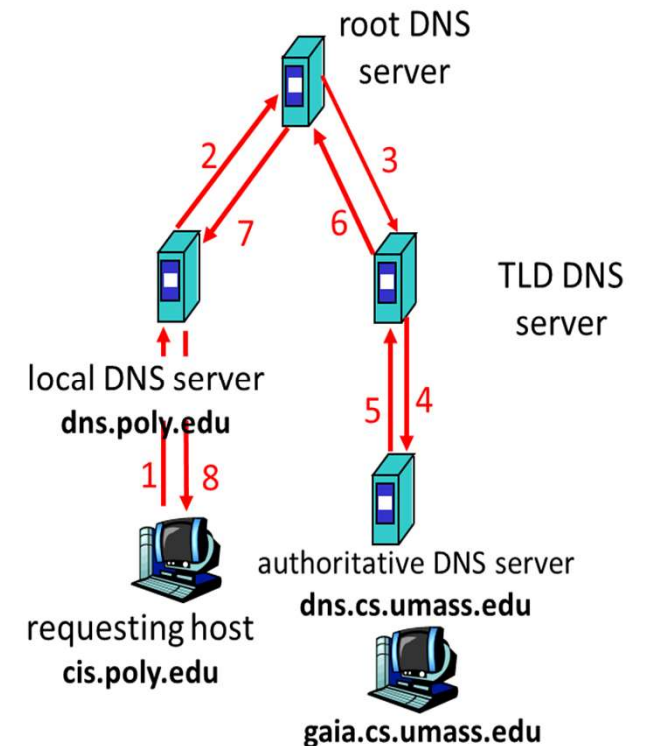
Consulta recursiva:

- El servidor DNS al que se pregunta es el encargado de resolver el nombre.

Búsqueda iterativa

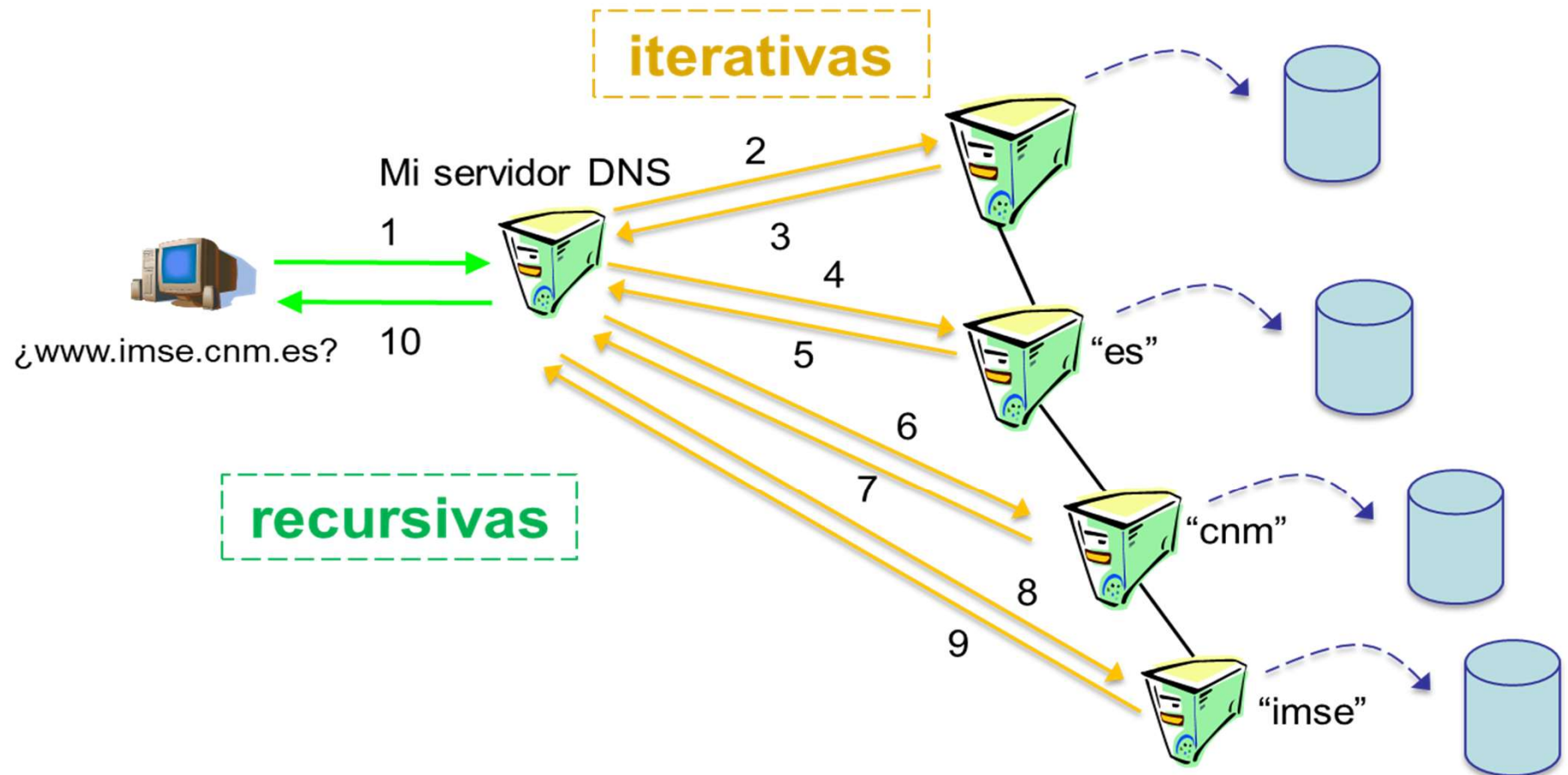


Búsqueda recursiva



Resolución de nombres DNS

- Tipos de consultas: iterativas vs recursivas

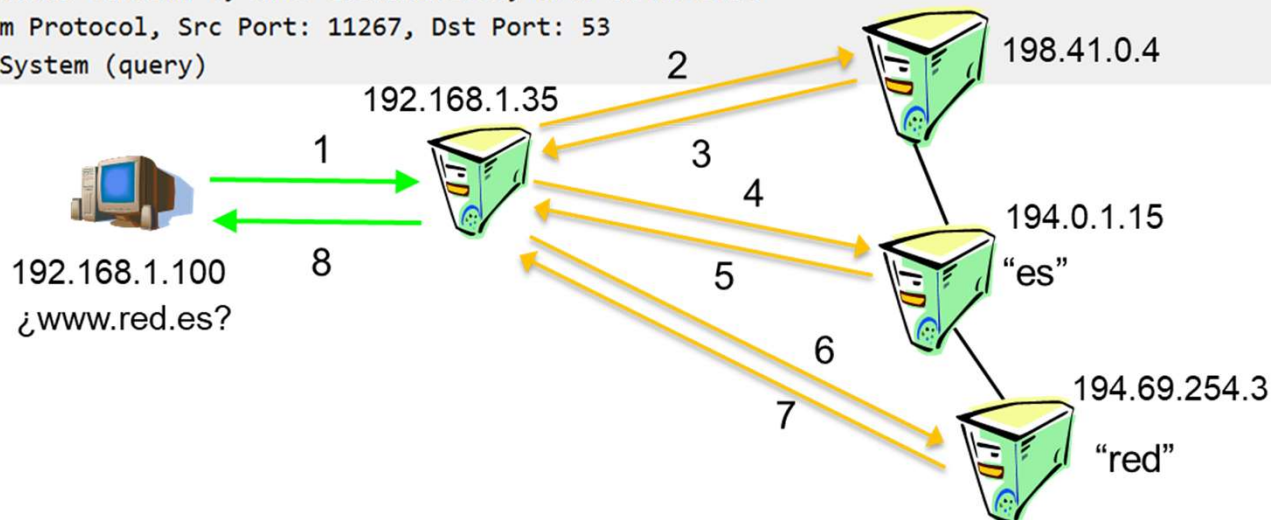


Resolución de nombres DNS

- Tipos de consultas: iterativas vs recursivas

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.100	192.168.1.35	DNS	70	Standard query 0x0003 A www.red.es
2	0.003141	192.168.1.35	198.41.0.4	DNS	81	Standard query 0x8c48 A www.red.es
3	0.099575	198.41.0.4	192.168.1.35	DNS	690	Standard query response 0x8c48 A ww
4	0.101291	192.168.1.35	194.0.1.15	DNS	81	Standard query 0x1276 A www.red.es
5	0.195829	194.0.1.15	192.168.1.35	DNS	269	Standard query response 0x1276 A ww
6	0.211829	192.168.1.35	194.69.254.3	DNS	81	Standard query 0x7584 A www.red.es
7	0.277134	194.69.254.3	192.168.1.35	DNS	249	Standard query response 0x7584 A ww
8	0.522270	192.168.1.35	192.168.1.100	DNS	172	Standard query response 0x0003 A ww

> Frame 12: 84 bytes on wire (672 bits), 84 bytes captured (672 bits) on interface unknown, id 0
> Ethernet II, Src: VMware_4a:31:cc (00:0c:29:4a:31:cc), Dst: ZyxelCom_52:e8:80 (c8:6c:87:52:e8:80)
> Internet Protocol Version 4, Src: 192.168.1.35, Dst: 194.0.1.15
> User Datagram Protocol, Src Port: 11267, Dst Port: 53
> Domain Name System (query)



Registros DNS

DNS: una base de datos distribuida almacena unos registros de recursos (**RR**)

Formato RR: (nombre, valor, tipo)

☐ Tipo=A

- **Nombre**: nombre del equipo
- **Valor**: dirección IP

☐ Tipo=NS

- **Nombre**: dominio (ej: ibm.com)
- **Valor**: nombre del servidor autoritativo para este dominio

☐ Tipo=CNAME

- **Nombre**: alias de algún nombre “canónico” (real)
(www.ibm.com es en realidad servereast.backup2.ibm.com)
- **Valor**: nombre canónico

☐ Tipo=MX

- **Valor**: nombre del servidor de correo asociado al nombre

Ejemplo: Inserción de RRs en DNS

- ❑ Ejemplo: creación nueva empresa “Network Utopia”, con nuevo dominio networkutopia.com
 - Paso 1: Registro del dominio networkutopia.com en un *registrador DNS* (ej., Network Solutions, responsable de los dominios .com)
 - Paso 2: proporcionar nombres y direcciones IP de los servidores autoritativos (principal y, opcionalmente, secundario/s). Se insertan, al menos, 2 RRs en el servidor TLD .com:
 - (networkutopia.com, dns1.networkutopia.com, NS)
 - (dns1.networkutopia.com, 212.212.212.2, A)
 - Paso 3: Añadir los recursos al servidor autoritativo (dns1.networkutopia.com) Por ejemplo, un servidor web en www.networkutopia.com y un servidor de correo.
 - (www.networkutopia.com, 212.212.212.3, A)
 - (networkutopia.com, mail.networkutopia.com, MX)
 - (mail.networkutopia.com, 212.212.212.4, A)

Ejemplo: RRs en zonas DNS

RRs en el servidor autoritativo de cnm.es

lmse.cnm.es.	IN	NS	ns.imse.cnm.es.
lmse.cnm.es.	IN	NS	ns2.imse.cnm.es.
ns.imse.cnm.es.	IN	A	150.214.7.6
ns2.imse.cnm.es.	IN	A	150.214.7.8

Lista de NS de la zona.

RRs en el servidor autoritativo de imse.cnm.es

\$ORIGIN imse.cnm.es.

\$TTL 172800

@ IN SOA ns.imse.cnm.es. postmaster.imse.cnm.es. (
2005050600 ; Serial
86400 ; Refresh 1 dia
7200 ; Retry 2 horas
2592000 ; Expire 30 dias
172800) ; Minimum 2 dias (172800)

; localhost entry. Se recomienda tener la entrada localhost.imse.cnm.es

localhost	IN	A	127.0.0.1
	IN	MX	100 mx.imse.cnm.es.
	IN	MX	200 mxback.imse.cnm.es.

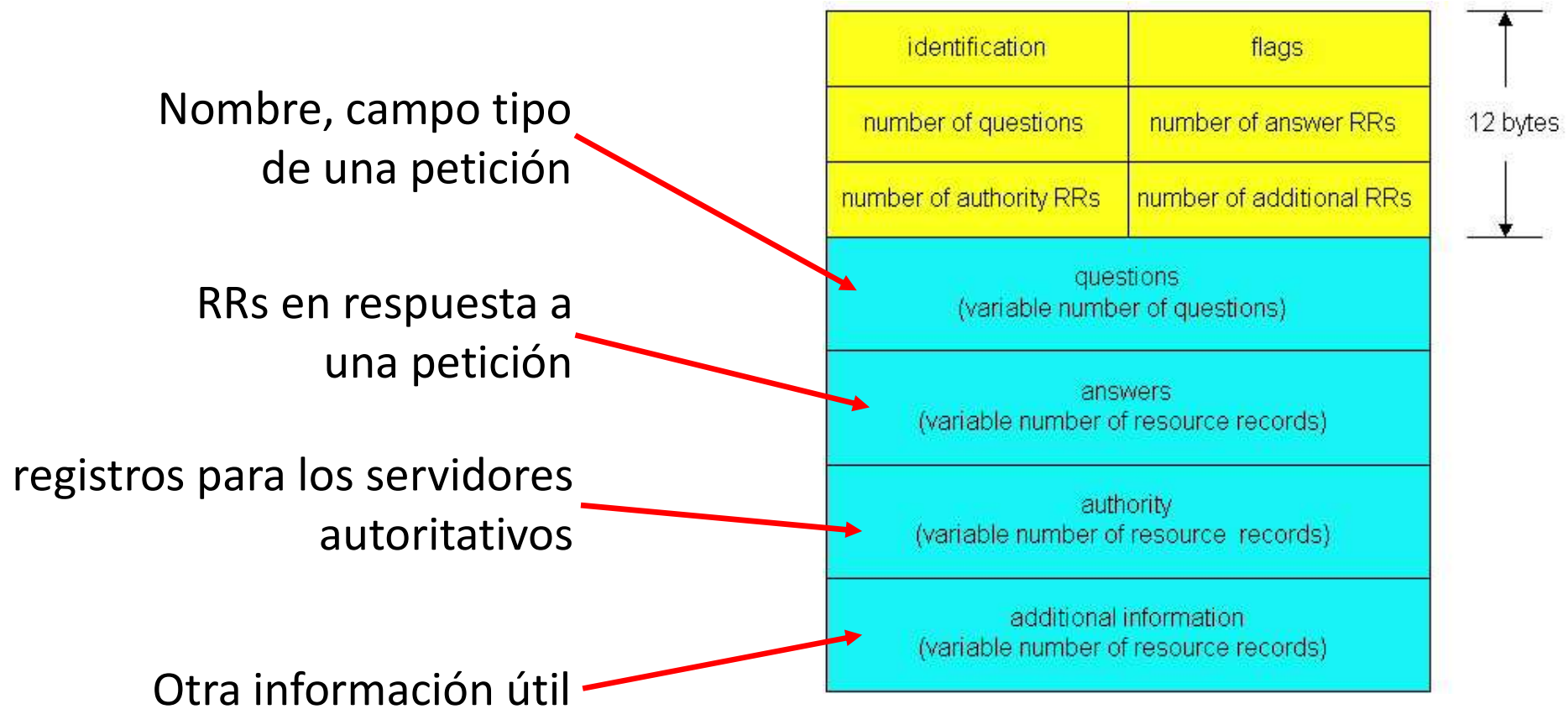
Registros MX, son los servidores de correo de la zona.

Entradas A, incluye una entrada localhost, y las de los MX.

mx	IN	A	150.214.7.5
mxback	IN	A	150.214.7.7
titan	IN	A	150.214.7.30.
www	IN	CNAME	titan
pop	IN	CNAME	titan
imap	IN	CNAME	titan
ns	IN	A	150.214.7.6
ns2	IN	A	150.214.7.8
lmse.cnm.es.	IN	NS	ns.imse.cnm.es.
lmse.cnm.es.	IN	NS	ns2.imse.cnm.es.

Estos son los alias de "titan"

Protocolo DNS, mensajes



DNS inverso

- ❑ Dada una IP -> Nombre de dominio
- ❑ Dominio especial **.arpa**
 - Subdominio .in-addr.arpa -> Traduce direcciones IPv4
 - Subdominio ip6.arpa -> Traduce direcciones IPv6
- ❑ Dominio in-addr.arpa
 - 4 etiquetas -> dígitos de la dirección... ¡al revés!
- ❑ Ejemplo: 196.141.214.150.in-addr.arpa obtiene el dominio que corresponde a la dirección 150.214.141.196
- ❑ Una petición DNS inversa devuelve un RR tipo PTR
- ❑ Herramienta **nslookup**

Servidores DNS primarios y secundarios

❑ Servidor primario

- Servidor principal (maestro).
- Datos originales de la zona DNS
- El administrador realiza las operaciones de alta y baja de nombres en él

❑ Servidor secundario

- Contienen una copia de la zona, generalmente obtenida del servidor primario
- Sirven como backups de los servidores primarios