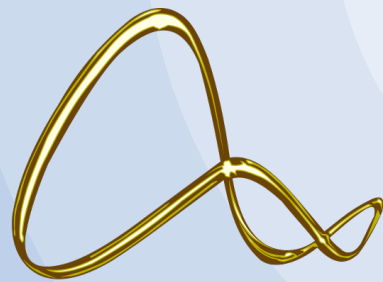


# CAPA DE APLICACIÓN

## *Protocolos de Internet 2TM8*

Gallegos Ruiz Diana Abigail

Montaño Mata América Itzel



upiita-ipn

2023

# Índice

<b>1</b>	<b>DHCP</b>	<b>3</b>
1.1	Función principal del protocolo . . . . .	3
1.2	Capa de Transporte utilizada . . . . .	3
1.3	Puertos utilizados . . . . .	3
1.4	Formato del paquete . . . . .	3
1.5	Tipos de asignación de direcciones . . . . .	5
1.5.1	Asignación estática de direcciones . . . . .	5
1.5.2	Asignación dinámica de direcciones . . . . .	5
1.6	Temporizadores . . . . .	5
1.7	Tipos de mensajes . . . . .	5
1.8	Diagrama de secuencia para la asignación de direcciones . . . . .	6
1.9	Mapa Conceptual . . . . .	7
<b>2</b>	<b>DNS</b>	<b>8</b>
2.1	Función principal del protocolo . . . . .	8
2.2	Capa de transporte utilizada . . . . .	8
2.3	Espacio de nombres . . . . .	8
2.4	Puertos utilizados . . . . .	9
2.5	Tipos de dominio . . . . .	9
2.6	Tipo de servidores . . . . .	10
2.7	Tipo de resoluciones . . . . .	10
2.8	Tipos de mensajes y sus campos . . . . .	12
2.9	Diagrama de secuencia para la resolución de nombre . . . . .	13
2.10	Mapa Conceptual . . . . .	14
<b>3</b>	<b>TELNET</b>	<b>15</b>
3.1	Función principal del protocolo . . . . .	15
3.2	Capa de transporte utilizada . . . . .	15
3.3	Puertos utilizados . . . . .	15
3.4	Uso de la Terminal Virtual de Red (NTV, Network Terminal Virtual) . . . . .	15
3.5	Tipo y función de los caracteres NTV . . . . .	15
3.6	Diagrama de establecimiento de sesión TELNET . . . . .	16
3.7	Tipos de opciones . . . . .	19
3.8	Modos de operación . . . . .	20
3.9	Comandos de usuario disponibles . . . . .	21
3.10	Mapa conceptual . . . . .	21
<b>4</b>	<b>FTP</b>	<b>23</b>
4.1	Función principal del protocolo . . . . .	23
4.2	Capa de transporte utilizada . . . . .	23
4.3	Puertos utilizados para establecer una sesión FTP . . . . .	23
4.4	Modelo básico FTP . . . . .	23
4.5	Tipos de conexiones existentes . . . . .	24
4.6	Componentes de un cliente FTP . . . . .	24
4.7	Componentes de un servidor FTP . . . . .	25

4.8	Problema de la heterogeneidad . . . . .	25
4.9	Atributos de comunicación . . . . .	25
4.10	Tipos de comando y su uso . . . . .	26
4.11	Tipos de códigos de respuesta . . . . .	29
4.12	Transferencia de archivos . . . . .	30
4.13	Mapa Conceptual . . . . .	31
<b>5</b>	<b>HTTP</b>	<b>32</b>
5.1	Función principal del protocolo . . . . .	32
5.2	Capa de transporte utilizada . . . . .	32
5.3	Puertos utilizados para establecer una sesión HTTP . . . . .	32
5.4	Significado y campos de un URL (Localizador Uniforme de Recursos) . . . . .	32
5.5	Tipos de mensajes y sus campos . . . . .	33
5.6	Métodos . . . . .	33
5.7	Códigos de respuesta o estado . . . . .	34
5.8	Diagramas de secuencia para una conexión persistente y una no persistente . . . . .	34
5.9	Uso de cookies . . . . .	35
5.10	Mapa Conceptual . . . . .	36
<b>6</b>	<b>SMTP,POP y IMAP4</b>	<b>37</b>
6.1	Función principal de cada protocolo . . . . .	37
6.2	Capa de transporte utilizada por cada uno de los protocolos . . . . .	37
6.3	Puertos utilizados para establecer una sesión SMTP . . . . .	37
6.4	Diagrama de secuencia para el establecimiento de sesión . . . . .	37
6.5	Función del Agente de Usuario (UA, User Agent) . . . . .	38
6.6	Función del Agente de transferencia de mensajes (MTA, Message Transfer Agent,) . . . . .	38
6.7	Formato de las direcciones de correo . . . . .	39
6.8	Mapa Conceptual . . . . .	41

# 1 DHCP

## 1.1 Función principal del protocolo

El protocolo de configuración dinámica de host (DHCP) es un protocolo cliente/servidor diseñado para proporcionar :

- La dirección IP de la computadora
- La máscara de subred de la computadora
- La dirección IP de un router
- La dirección IP de un servidor de nombres

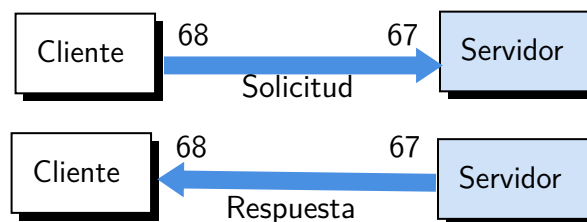
para una computadora sin disco o un computador que se inicia por primera vez.

## 1.2 Capa de Transporte utilizada

Utiliza el protocolo de transporte UDP para la transmisión de sus mensajes.

## 1.3 Puertos utilizados

El servidor utiliza el puerto conocido 67, que es el normal. El cliente utiliza el conocido puerto 68, que es inusual.



**Figura 1:** Uso de los puertos UDP

## 1.4 Formato del paquete

A continuación se muestra el formato del paquete para el protocolo DHCP:

- **Código de operación:** Indica solicitud (1) o respuesta (2).
- **Tipo de hardware:** Indica el tipo de hardware. Por ejemplo 1 indica Ethernet.
- **Longitud de Hardware:** Indica la longitud en bytes de la dirección física.
- **Cuenta de saltos:** define el número máximo de saltos que el paquete puede viajar.
- **Identificador de transacción:** es establecido por el cliente y se utiliza para hacer coincidir una respuesta con la solicitud. El servidor devuelve el mismo valor en su respuesta.

**Tabla 1:** Formato del paquete

0	8	16	24	31
Código de operación	Tipo de Hardware	Longitud de Hardware	Cuenta de Saltos	de
Identificador de transacción				
Tiempo (# Segundos)		Banderas		
Dirección IP del cliente				
Dirección IP asignada				
Dirección IP del servidor				
Dirección IP del gateway				
Dirección hardware del cliente				16 bytes
Nombre del servidor				64 bytes
Nombre del archivo arranque				128 bytes
Opciones				Variable

- **Tiempo:** indica en segundos, el tiempo transcurrido desde el inicio del cliente.
- **Banderas:** El bit más significativo de este campo se utiliza como indicador de broadcast (1) o unicast (0) . El resto de bits deben fijarse a 0.
- **Dirección IP del cliente:**Establecido por el cliente, indica su dirección IP, en caso de que no la conozca, deja vacío este campo.
- **Dirección IP asignada:** contiene la dirección IP del client, rellenado por el servidor (en el mensaje de respuesta) a petición del cliente.
- **Dirección IP del servidor:**contiene la dirección IP del servidor, es rellenado por el mismo en un mensaje de respuesta.
- **Dirección IP del gateway:** contiene la dirección IP de un router, es rellenado por el servidor en un mensaje de respuesta.
- **Dirección hardware del cliente:** dirección física del cliente.
- **Nombre del servidor:** se rellena opcionalmente, contiene una cadena terminada en cero formada por el nombre de dominio del servidor.
- **Nombre del archivo de arranque:** se rellena opcionalmente, contiene una cadena terminada en cero que consiste en la ruta completa del archivo de arranque. El cliente puede utilizar esta ruta para recuperar otra información de arranque.

- **Opciones:** Información adicional que solo se utiliza en los mensajes de respuesta. Una opción se compone de tres campos: un campo de etiqueta de 1 byte, un campo de longitud de 1 byte y un campo de valor de longitud variable.

## 1.5 Tipos de asignación de direcciones

### 1.5.1 Asignación estática de direcciones

Sucede cuando un servidor DHCP tiene una base de datos que vincula estáticamente direcciones físicas a direcciones IP. En esta modalidad, DHCP es compatible con el protocolo obsoleto BOOTP.

### 1.5.2 Asignación dinámica de direcciones

DHCP tiene una segunda base de datos con un pool de direcciones IP disponibles. Cuando un cliente DHCP solicita una dirección IP temporal, el servidor DHCP va al pool de direcciones IP disponibles (no utilizadas) y asigna una dirección IP por un periodo de tiempo negociable. Cuando un cliente DHCP envía una solicitud a un servidor DHCP, el servidor comprueba primero su base de datos estática. Si existe una entrada con la dirección física solicitada en la base de datos estática, se devuelve la dirección IP permanente del cliente. Por otro lado, si la entrada no existe en la base de datos estática, el servidor selecciona una dirección IP del pool disponible, asigna la dirección al cliente y añade la entrada a la base de datos dinámica.

El servidor DHCP emite un arrendamiento por un periodo de tiempo específico. Cuando el contrato expira, el cliente debe dejar de usar la dirección IP o renovar el contrato. El servidor tiene la opción de aceptar o rechazar la renovación. Si el servidor no está de acuerdo, el cliente deja de utilizar la dirección. dirección.

## 1.6 Temporizadores

El cliente utilice tres tiempos: temporizador de renovación, temporizador de rebinding y temporizador de expiración. Si el servidor no especifica los valores de tiempo de espera para estos temporizadores cuando la dirección es asignada, el cliente necesita usar el valor por defecto que se muestra a continuación:

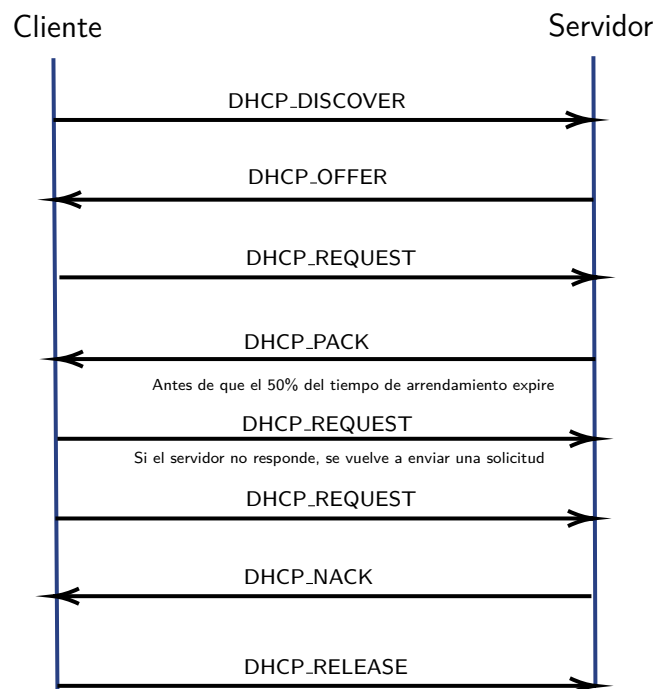
<b>Temporizador de renovación:</b>	50% del tiempo de arrendamiento
<b>Temporizador de rebinding:</b>	87.5% del tiempo de arrendamiento
<b>Temporizador de caducidad:</b>	100% del tiempo de arrendamiento

## 1.7 Tipos de mensajes

- **DHCP\_DISCOVER:** Mensaje de difusión enviado por un cliente DHCP para solicitar que algún servidor DHCP de la red le envíe los parámetros de configuración de red.
- **DHCP\_OFFER:** Enviado por un servidor DHCP en respuesta a un mensaje DHCP\_DISCOVER de un cliente. El servidor ofrece en el mensaje una concesión de una IP junto con valores para los parámetros solicitados por el cliente.
- **DHCP\_REQUEST:** Enviado por un cliente en respuesta a un mensaje DHCP\_OFFER recibido desde un servidor o bien cada vez que el cliente tiene que renovar una concesión. El cliente indica al servidor que acepta la oferta hecha por el servidor y solicita que le otorgue una concesión de la IP.

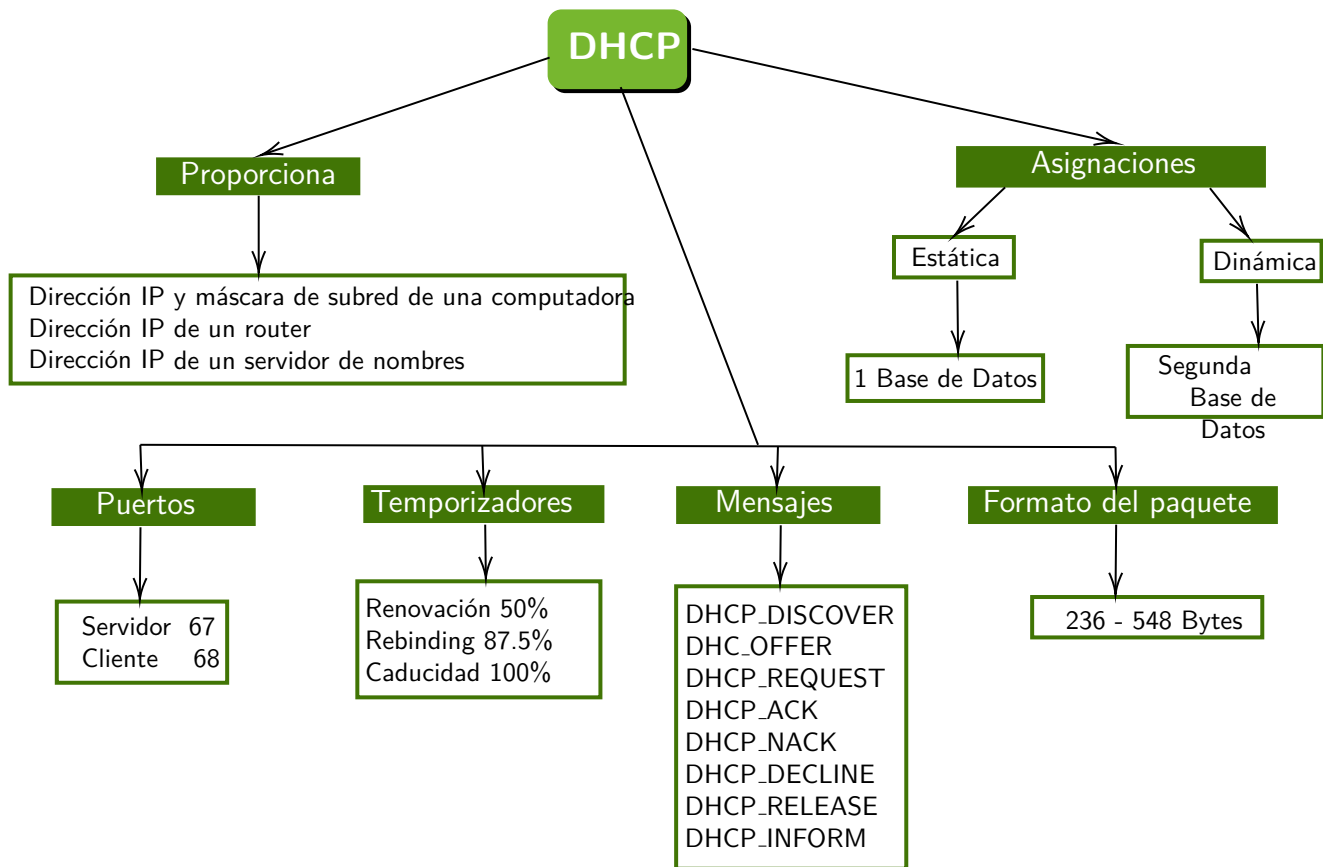
- **DHCP\_ACKnowledge:** Enviado por el servidor a un cliente en respuesta a un mensaje DHCP\_REQUEST. Se indica al cliente que le asigna la IP solicitada durante un tiempo de concesión establecido.
- **DHCP\_NAK:** Enviado desde un servidor a un cliente en respuesta a un mensaje DHCP\_REQUEST para indicarle que no puede entregarle la IP que ha solicitado en ese mensaje .
- **DHCP\_DECLINE:** EEnviado por cliente DHCP en sustitución de un mensaje DHCP\_REQUEST cuando detecta que la IP que se le ha ofrecido ya está siendo usada en la red.
- **DHCP\_RELEASE:** Enviado por el cliente DHCP al servidor para indicar una concesión terminada .
- **DHCP\_INFORM:** EEnviado por el cliente DHCP al servidor para solicitarle parámetros adicionales de configuración de red . [1]

## 1.8 Diagrama de secuencia para la asignación de direcciones



**Figura 2:** Diagrama de secuencia. Adaptada de *TCP/IP Protocol-suite* (ed. 4,p.579), por B. Forouzan

## 1.9 Mapa Conceptual





## 2 DNS

### 2.1 Función principal del protocolo

El Sistema de Nombres de Dominio (DNS) es una aplicación cliente-servidor que identifica a cada host en Internet con un nombre único y fácil de usar. El DNS organiza el espacio de nombres en una estructura jerárquica para descentralizar las responsabilidades implicadas en la asignación de nombres.[2]

### 2.2 Capa de transporte utilizada

DNS puede utilizar UDP o TCP.

- Si el servidor de resolución sabe de antemano que el tamaño del mensaje de respuesta es superior a 512 bytes, utiliza la conexión TCP.
- Si el servidor de resolución no conoce el tamaño del mensaje de respuesta, puede utilizar el puerto UDP

### 2.3 Espacio de nombres

Para ser inequívocos, los nombres asignados a las máquinas deben ser únicos porque las direcciones IP son únicas. Un espacio de nombres que asigna cada dirección a un nombre único puede organizarse de dos maneras: plana o jerárquica.

En un **espacio de nombres jerárquico**, cada nombre se compone de varias partes. La primera parte puede definir la naturaleza de la organización, la segunda parte puede definir el nombre de una organización, la tercera parte puede definir los departamentos de la organización, etc.

#### Etiqueta

Cada nodo del árbol tiene una etiqueta, que es una cadena con un máximo de 63 caracteres. La etiqueta **root** es una cadena nula (cadena vacía). DNS exige que los hijos de un nodo tengan etiquetas diferentes, lo que garantiza la unicidad de los nombres de dominio.

#### Nombre de dominio

Cada nodo del árbol tiene un nombre de dominio. Un nombre de dominio completo es una secuencia de etiquetas separadas por puntos (.). Los nombres de dominio se leen siempre desde el nodo hasta la raíz. La última etiqueta es la etiqueta de la raíz (null). Esto significa que un nombre de dominio completo siempre termina en una etiqueta null, lo que significa que el último carácter es un punto porque la cadena null es nada.

**Nombre de dominio totalmente cualificado (FQDN)** Si una etiqueta termina con una cadena nula, se denomina nombre de dominio completo (FQDN), contiene el nombre completo de un host. En otras palabras, contiene todas las etiquetas, desde las más específicas a las más generales, que definen de forma única el nombre del host.

**Nombre de dominio parcialmente cualificado (PQDN)** Si una etiqueta no termina con una cadena nula se denomina nombre de dominio parcialmente cualificado (PQDN). Un PQDN parte de un nodo, pero no llega a la raíz. Se utiliza cuando el nombre que hay que resolver pertenece al mismo sitio que el cliente.

## 2.4 Puertos utilizados

En ambos casos el puerto utilizado por el servidor es el puerto 53.

## 2.5 Tipos de dominio

**Un dominio** es un subárbol del espacio de nombres de dominio. El nombre del dominio es el nombre del nodo que encabeza el subárbol.

El espacio de nombres de dominio se divide en tres secciones diferentes: dominios genéricos, dominios de países y dominios inversos.

### Dominios genéricos

Define los hosts registrados según su comportamiento genérico. Cada nodo de un árbol define el nombre de dominio, que es un índice de la base de datos DNS. Utiliza etiquetas de tres caracteres, y estas etiquetas describen el tipo de organización. Véase 2.

**Tabla 2:** Etiquetas comunes

aero	Compañías aéreas y aeroespaciales
biz	Negocios o empresas
com	Organizaciones comerciales
coop	Organizaciones empresariales cooperativas
edu	Instituciones educativas
gov	Instituciones gubernamentales
info	Proveedores de servicios de información
int	Organizaciones internacionales
mil	Grupos militares
museum	Museo y otras organizaciones sin ánimo de lucro
name	Nombres personales
net	Red Centros de apoyo
org	Organizaciones sin ánimo de lucro
pro	Organizaciones profesionales individuales

### Dominios de países

El formato del dominio de país es el mismo que el de un dominio genérico, pero utiliza abreviaturas de dos caracteres (por ejemplo, us para Estados Unidos).

## Dominios inversos

El dominio inverso se utiliza para asignar una dirección a un nombre. Cuando el servidor ha recibido una solicitud del cliente, y el servidor contiene los archivos de sólo los clientes autorizados. Para determinar si el cliente está en la lista de autorizados o no, envía una solicitud al servidor DNS y pide la asignación de una dirección al nombre. [3]

## 2.6 Tipo de servidores

**Zona:** Lo que un servidor es responsable o sobre lo que tiene autoridad se denomina zona. Podemos definir una zona como una parte contigua de todo el árbol.

### Servidor root

Un servidor root es un servidor cuya zona está formada por todo el árbol. Normalmente no almacena ninguna información sobre dominios, sino que delega su autoridad en otros servidores, manteniendo referencias a ellos. están distribuidos por todo el mundo.

### Servidores primarios

Un servidor primario es un servidor que almacena un archivo en un disco local sobre la zona de la que es autoridad. Es responsable de crear, mantener y actualizar el archivo de zona.

### Servidores secundarios

Un servidor secundario es un servidor que transfiere la información completa sobre una zona desde otro servidor (primario o secundario) y almacena el archivo en su disco local. El servidor secundario no crea ni actualiza los archivos de zona. Si es necesario actualización, debe realizarla el servidor primario, que envía la versión actualizada al secundario.

Tanto el servidor primario como el secundario son autoritativos para las zonas que sirven. Al usar ambos, se busca crear redundancia para los datos, de modo que si un servidor falla, el otro pueda seguir sirviendo a los clientes. Un servidor puede ser primario para una zona específica y secundario para otra.[4]

## 2.7 Tipo de resoluciones

La asignación de un nombre a una dirección o de una dirección a un nombre se denomina **resolución nombre-dirección**. Un host que necesita asignar una dirección a un nombre o un nombre a una dirección llama a un cliente DNS llamado **resolver**.

### Resolución recursiva

El resolver (cliente) espera que el servidor proporcione la respuesta final. Si el servidor es la autoridad para el nombre de dominio, comprueba su base de datos y responde. Por el contrario, envía la petición a otro servidor (normalmente el servidor padre) y espera la respuesta. Si el padre es la autoridad, responde; de lo contrario, envía la solicitud a otro servidor. Cuando finalmente se resuelve la solicitud, la respuesta se devuelve hasta que llega al cliente solicitante.

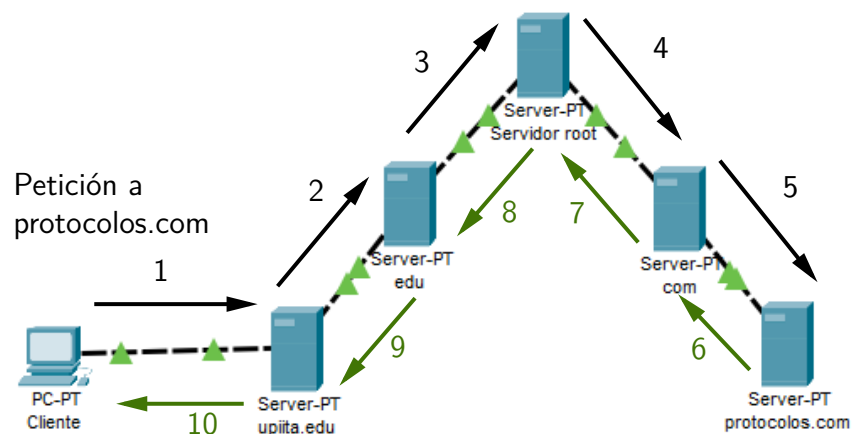


Figura 3: Resolución recursiva

## Resolución iterativa

Si el servidor es una autoridad para el nombre, envía la respuesta. Si no lo es, devuelve (al cliente) la dirección IP del servidor que cree que puede resolver la solicitud. Se denomina iterativo porque el cliente repite la misma solicitud a varios servidores.

Petición a protocolos.com

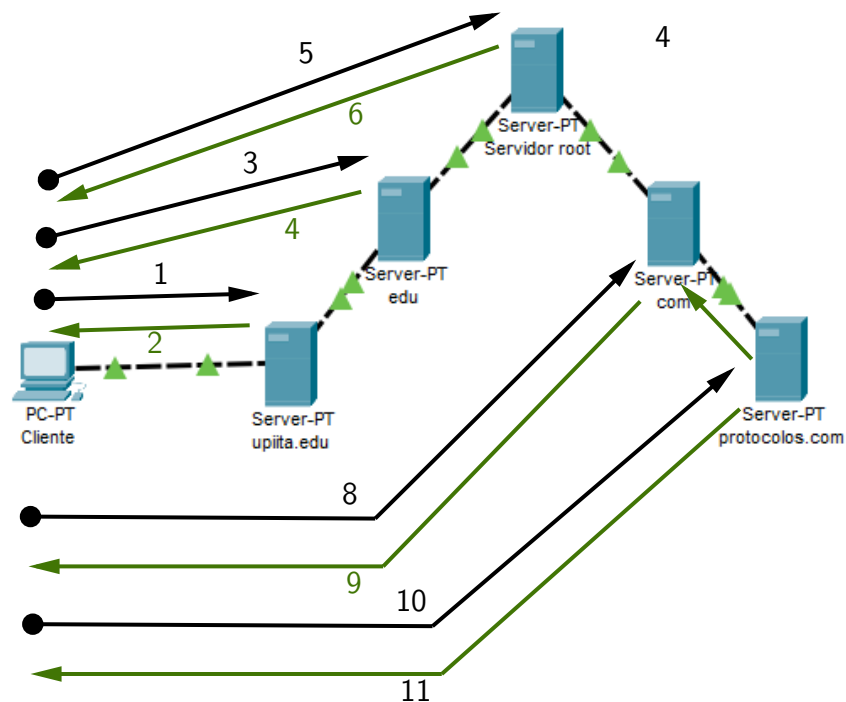


Figura 4: Resolución iterativa

## 2.8 Tipos de mensajes y sus campos

DNS tiene dos tipos de mensajes: consulta y respuesta. Ambos tipos tienen el mismo formato. El mensaje de consulta consta de un encabezado y registros de preguntas; el mensaje de respuesta consta de un encabezado, registros de preguntas, registros autorizados y registros adicionales.

### Encabezado

Tanto los mensajes de consulta como los de respuesta tienen el mismo formato de encabezado con algunos campos establecidos a cero para los mensajes de consulta.

**Tabla 3:** Formato del encabezado

Identificación	Banderas
Número de registros de preguntas.	Número de registros de respuesta (Todos los 0 en el mensaje de consulta).
Número de registros autorizados (Todos los 0 en el mensaje de consulta).	Número de registros adicionales (Todos los mensajes de consulta).

**Identificación.** Campo de 16 bits utilizado por el cliente para hacer coincidir la respuesta con la consulta. El cliente utiliza un número de identificación diferente cada vez que envía una consulta. El servidor duplica este número en la respuesta correspondiente.

**Banderas.** Campo de 16 bits que consta de los siguientes subcampos.

**Tabla 4:** Banderas

QR	OpCode	AA	TC	RD	RA	000	rCode
----	--------	----	----	----	----	-----	-------

- **QR**(consulta/respuesta). Este es un subcampo de 1 bit que define el tipo de mensaje. Si es 0, el mensaje es una consulta. Si es 1, el mensaje es una respuesta.
- **OpCode** (*código de operación*) . Este es un subcampo de 4 bits que define el tipo de consulta o respuesta (0 si es estándar, 1 si es inversa y 2 si es una solicitud de estado del servidor).
- **AA**(respuesta autorizada). Este es un subcampo de 1 bit. Cuando se establece (valor de 1) significa que el servidor de nombres es un servidor autorizado. Se usa solo en un mensaje de respuesta.
- **TC** (*Truncado*) Este es un subcampo de 1 bit. Cuando se establece (valor de 1), significa que la respuesta era de más de 512 bytes y se truncó a 512. Se utiliza cuando DNS utiliza los servicios de UDP.
- **RD** (*recursión deseada*) Este es un subcampo de 1 bit. Cuando se establece (valor de 1)significa que el cliente desea una respuesta recursiva. Se establece en el mensaje de consulta y repetición en el mensaje de respuesta.

- *RA* (recurrencia disponible). Este es un subcampo de 1 bit. Cuando se establece en la respuesta, significa que una respuesta recursiva está disponible. Se establece sólo en la respuesta del mensaje.
- *Reserved* (*reservado*). subcampo de 3 bits establecido en 000.
- *rCode*. campo de 4 bits que muestra el estado del error en la respuesta (solo para servidores autorizados).

## 2.9 Diagrama de secuencia para la resolución de nombre

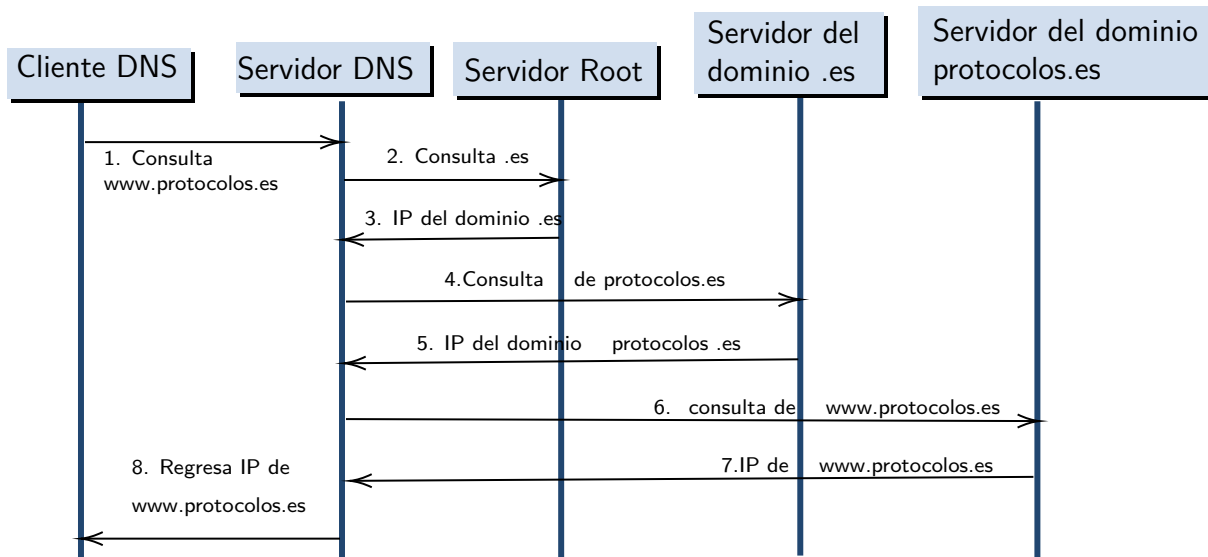


Figura 5: Resolución iterativa

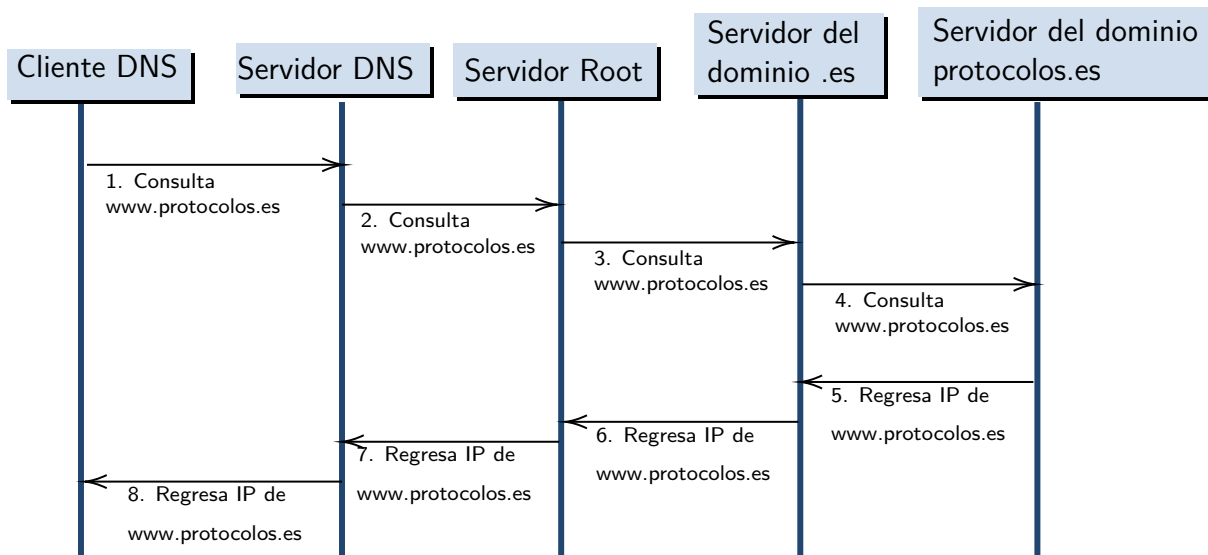
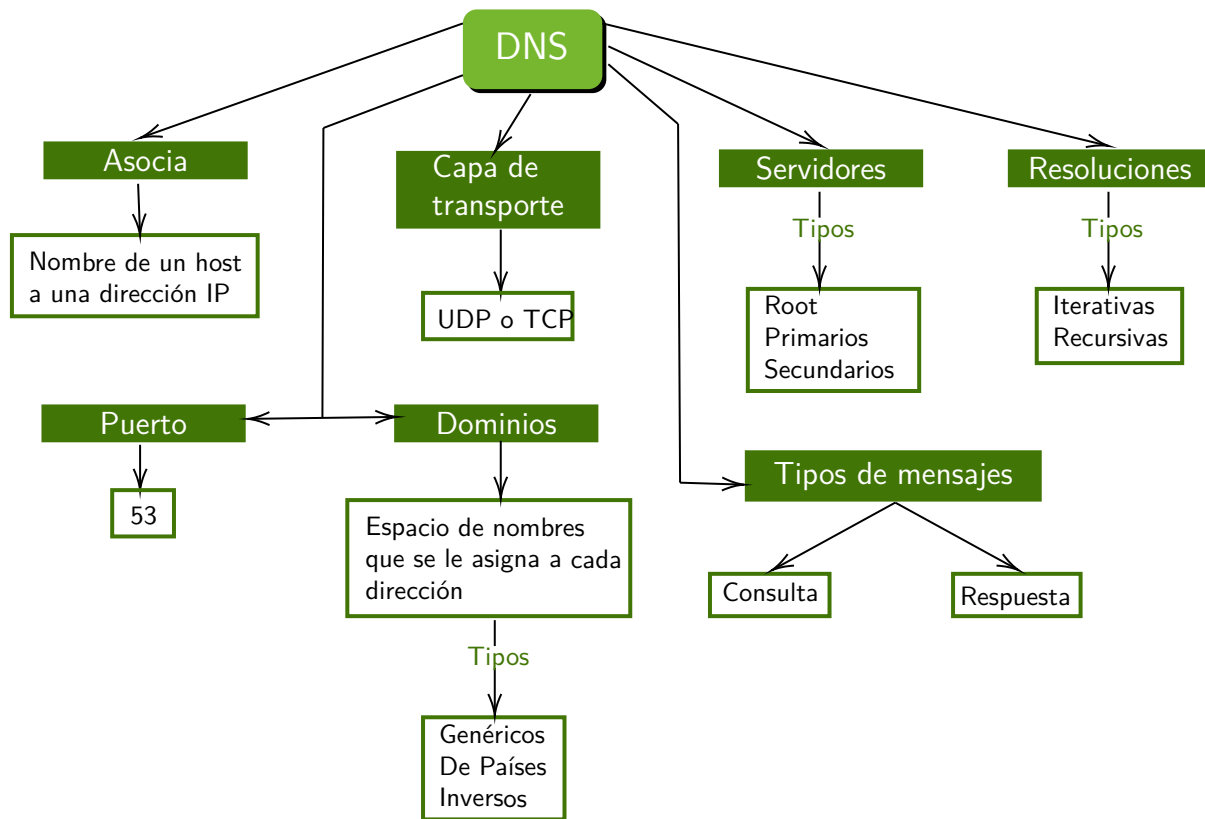


Figura 6: Resolución Recursiva

## 2.10 Mapa Conceptual



## 3 TELNET

### 3.1 Función principal del protocolo

TELNET es una aplicación cliente-servidor que permite a un usuario conectarse a una máquina remota.

### 3.2 Capa de transporte utilizada

TELNET utiliza TCP como su protocolo de capa de transporte.

### 3.3 Puertos utilizados

El servidor TELNET escucha en el puerto bien conocido TCP 23. [5]

### 3.4 Uso de la Terminal Virtual de Red (NTV, Network Terminal Virtual)

Al tratar con sistemas heterogéneos, se debe saber a qué tipo de computadora nos vamos a conectar, y también debemos instalar el emulador de terminal específico que utiliza ese ordenador. TELNET resuelve este problema definiendo una interfaz universal llamada **Network Virtual Network Virtual Terminal (NVT)**. A través de esta interfaz, el cliente TELNET traduce los caracteres (datos o comandos) procedentes del terminal local en forma NVT y los envía a la red. El servidor TELNET, por su parte, traduce los datos y comandos del formato NVT al formato aceptable por la computadora remota.

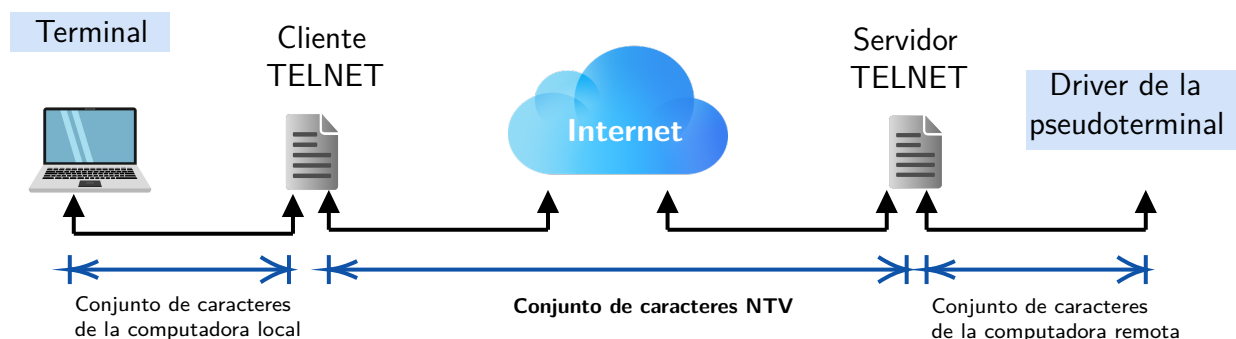


Figura 7: Concepto de NTV

### 3.5 Tipo y función de los caracteres NTV

NVT utiliza dos conjuntos de caracteres, uno para datos y otro para control. Ambos son bytes de 8 bits.

#### Caracteres de datos

Para datos, NVT normalmente usa NVT ASCII. Esto es un conjunto de caracteres de 8 bits en el que los siete bits de menor orden son los mismos que los del ASCII de EE. UU. y el bit de mayor orden es 0. Aunque es



posible enviar un ASCII de 8 bits (con el bit de mayor orden establecido en 0 o 1), primero debe acordarse entre el cliente y el servidor mediante la negociación de opciones.

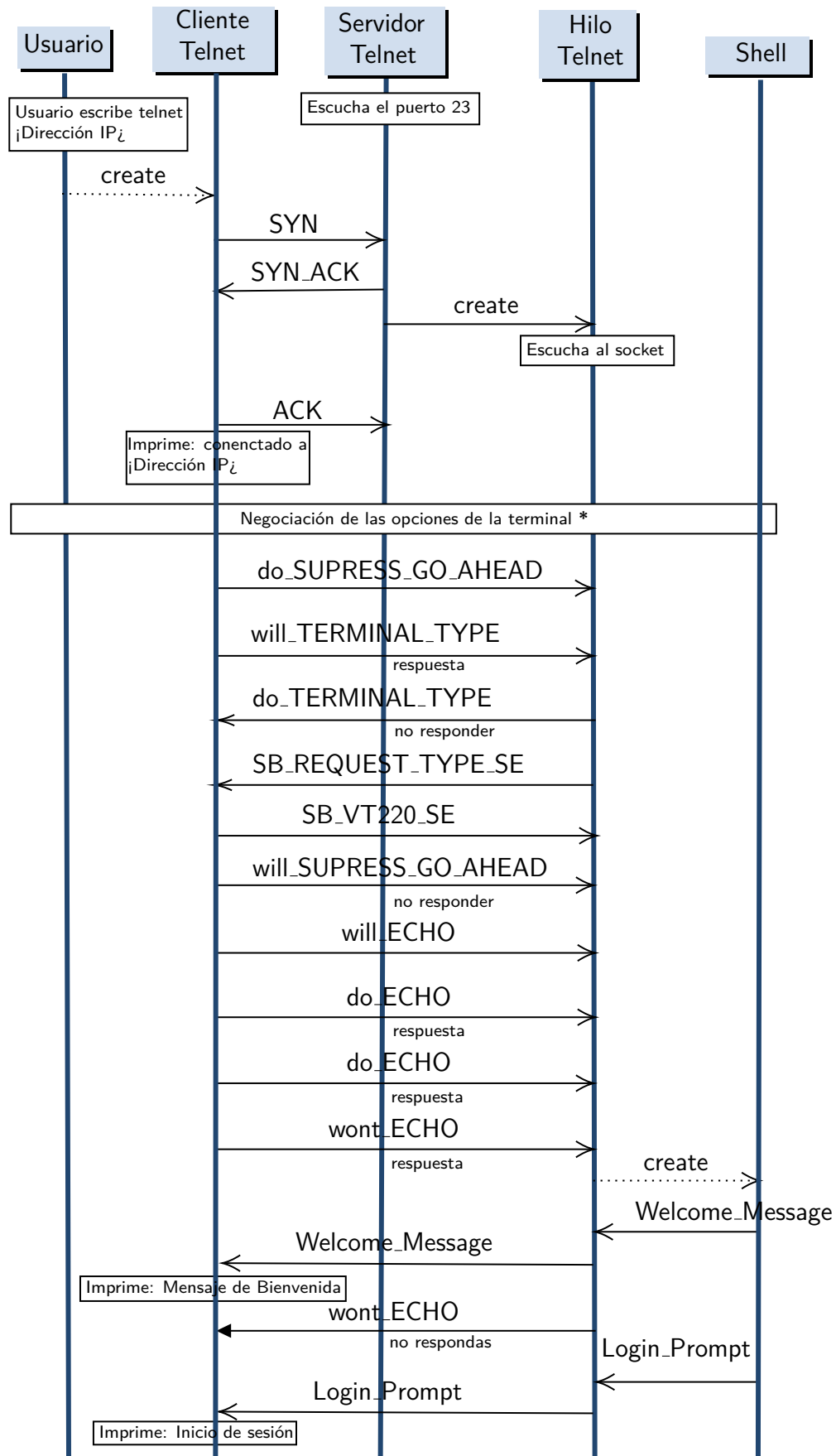
## Caracteres de control

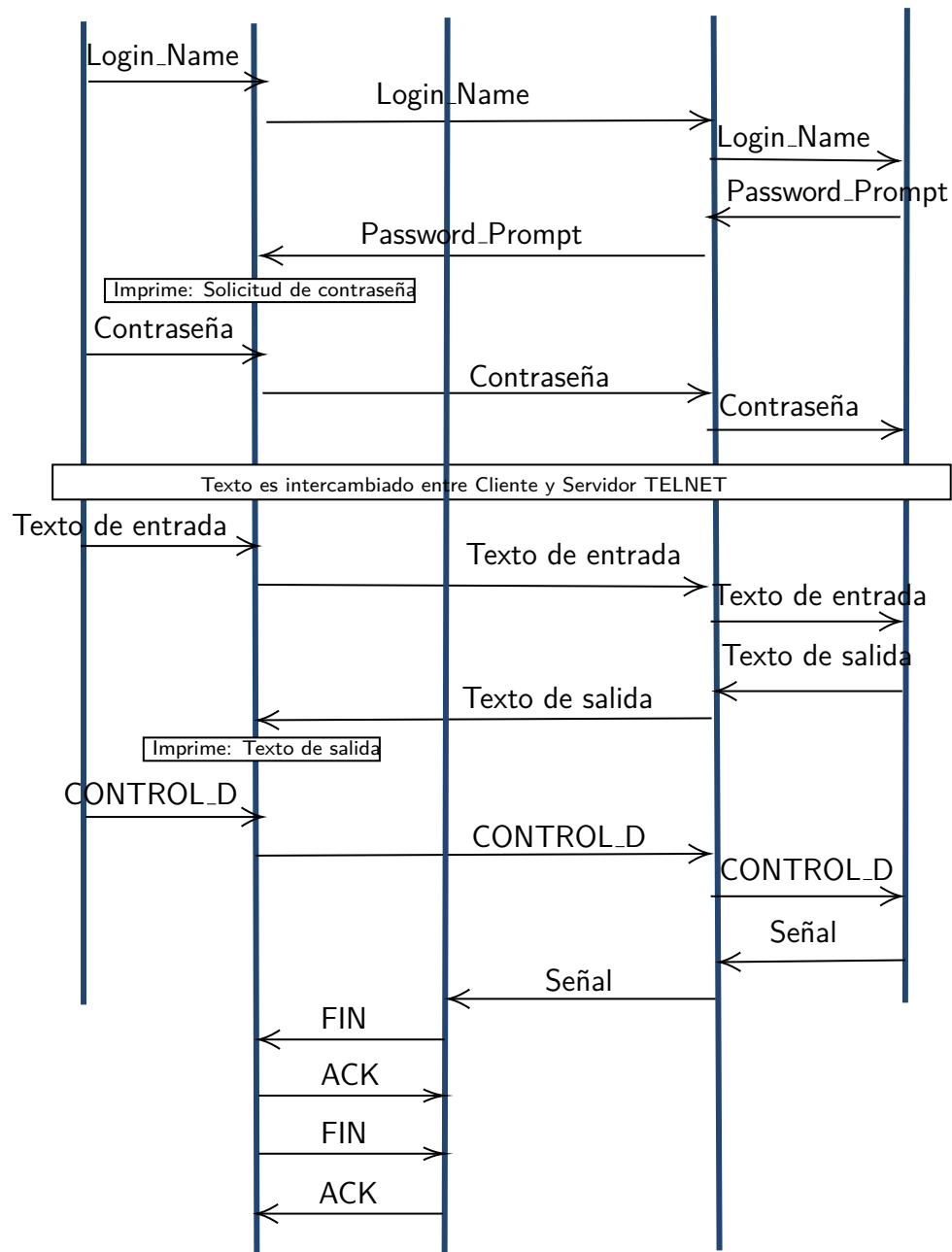
Para enviar caracteres de control entre computadoras (del cliente al servidor o viceversa), NVT utiliza un conjunto de caracteres de 8 bits en el que se establece el bit de mayor orden a 1.

**Tabla 5:** Caracteres comunes de NTV

Carácter	Decimal	Binario	Significado
EOF	236	11101100	Fin del documento.
EOR	239	11101111	Finde registro.
SE	240	11110000	Fin de la sub-opción.
NOP	241	11110001	No operación.
DM	242	11110010	Marca de datos.
BRK	243	11110011	Romper.
IP	244	11110100	Proceso de interrupción
AO	245	11110101	Abortarsalida.
AYT	246	11110110	¿Está ahí?
EC	247	11110111	Borrar carácter.
EL	248	11111000	Borrar línea.
GA	249	11111001	Avanzar.
SB	250	11111010	Comienzo de la sub-opción.
WILL	251	11111011	Acuerdo para habilitar la opción.
WONT	252	11111100	Negativa a habilitar la opción.
DO	253	11111101	Aprobación de solicitud de opción.
DONT	254	11111110	Negación de solicitud de opción.
IAC	255	11111111	Interpretar (el siguiente carácter) como control.

## 3.6 Diagrama de establecimiento de sesión TELNET





**Figura 8:** Diagrama de secuencia TELNET Adaptado de: [6]

**Nota\*:** Telnet utiliza los comandos "will", "won't", "do" y "don't" para negociar opciones entre el cliente y el servidor.

- **"Will"** muestra el deseo de usar, o la confirmación de utilizar la opción indicada por el código inmediatamente siguiente.
- **"Won't"** muestra el rechazo a utilizar o continuar utilizando la opción.
- **"Do"** solicita que la otra parte utilice o confirma que espera que la otra parte utilice la opción indicada por el código inmediatamente siguiente.
- **"No"** exige que la otra parte deje de utilizar, o confirma que usted ya no espera que la otra parte utilice, la opción indicada por el código inmediatamente siguiente.[6]

### 3.7 Tipos de opciones

TELNET permite que el cliente y el servidor negocien opciones antes o durante el uso del servicio. La siguiente tabla muestra algunas opciones comunes:

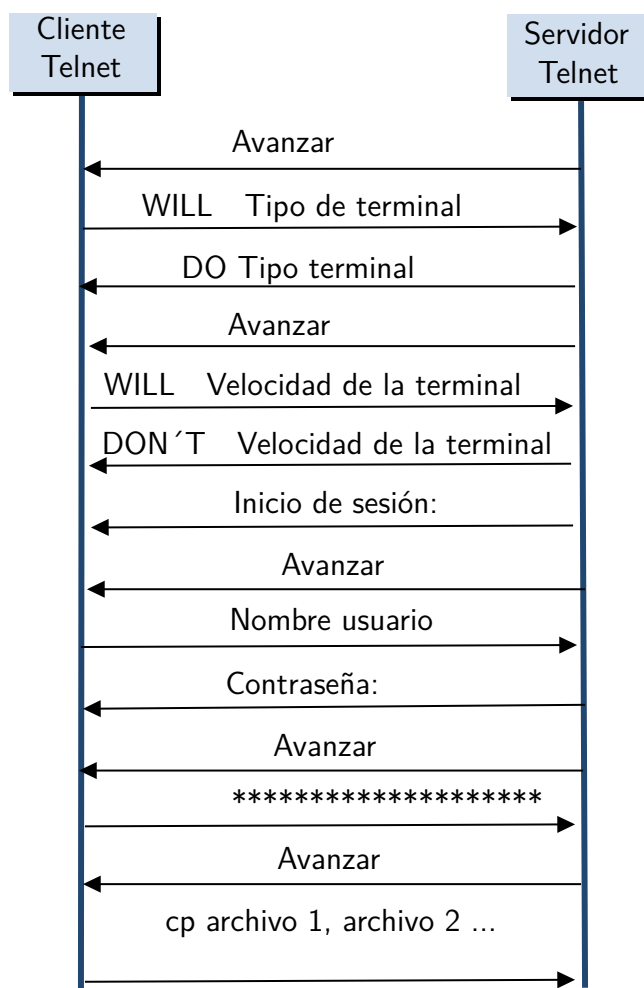
**Tabla 6:** Tipos de opciones

Código	Significado	
0	Binario	Interpreta como transmisión binaria de 8 bits
1	Echo	Hacer Echo de los datos recibidos de un lado al otro
3	Suprimir el visto bueno	Suprimir las señales de visto bueno después de los datos
5	Status	Solicitar el estado de TELNET
6	Marca de tiempo	Definir las marcas de tiempo.
24	Tipo de terminal	Establecer el tipo de terminal.
32	Velocidad terminal	Establecer la velocidad terminal.
34	Modo de línea	Cambiar al modo de línea.

## 3.8 Modos de operación

### Modo por defecto

El modo por defecto se utiliza si no se invocan otros modos a través de la negociación de opciones. En este modo, el eco lo hace el cliente. El usuario escribe un carácter y el cliente hace eco del carácter en la pantalla (o en la impresora) pero no lo envía hasta que se haya completado una línea entera. Después, el cliente espera la orden GA forward) del servidor antes de aceptar una nueva línea del usuario. El funcionamiento es semidúplex pero no es eficaz en TCP por lo que este modo se está quedando obsoleto.



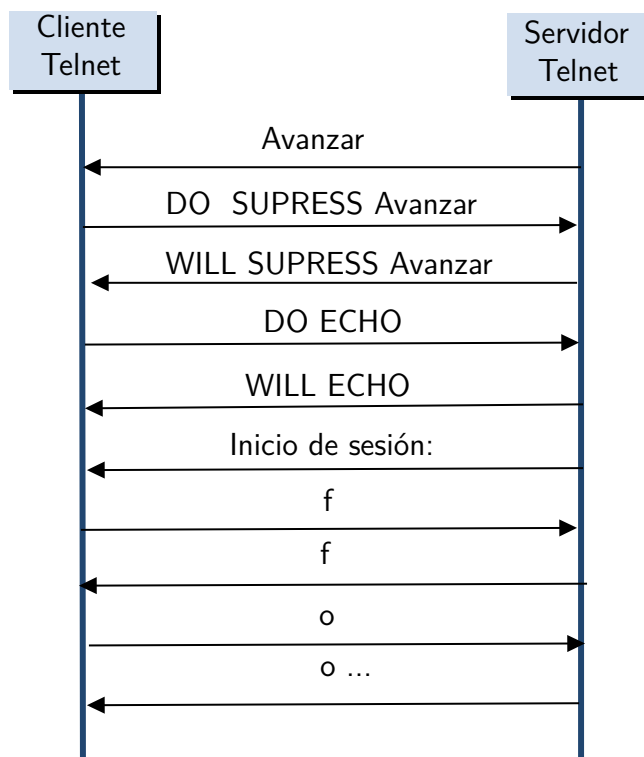
**Figura 9:** Diagrama de secuencia del modo por defecto

### Modo carácter

En el modo carácter, cada carácter tecleado es enviado por el cliente al servidor. En este modo, el eco del carácter puede retrasarse si el tiempo de transmisión es largo. También crea tráfico para la red porque deben enviarse tres segmentos TCP por cada carácter de datos:

1. El usuario introduce un carácter que se envía al servidor.
2. El servidor acusa recibo y devuelve el carácter (en un segmento).

3. El cliente acusa recibo del carácter enviado.



**Figura 10:** Diagrama de secuencia del modo carácter

## Modo Línea

Es un nuevo modo propuesto, en donde la edición de línea (eco, borrado de caracteres, borrado de líneas, etc.) la realiza el cliente. A continuación, el cliente envía la línea completa al servidor. El modo por defecto funciona en modo half-duplex; el modo de línea es full-duplex con el cliente enviando una línea tras otra, sin necesidad de que intervenga un carácter GA (adelante) del servidor.

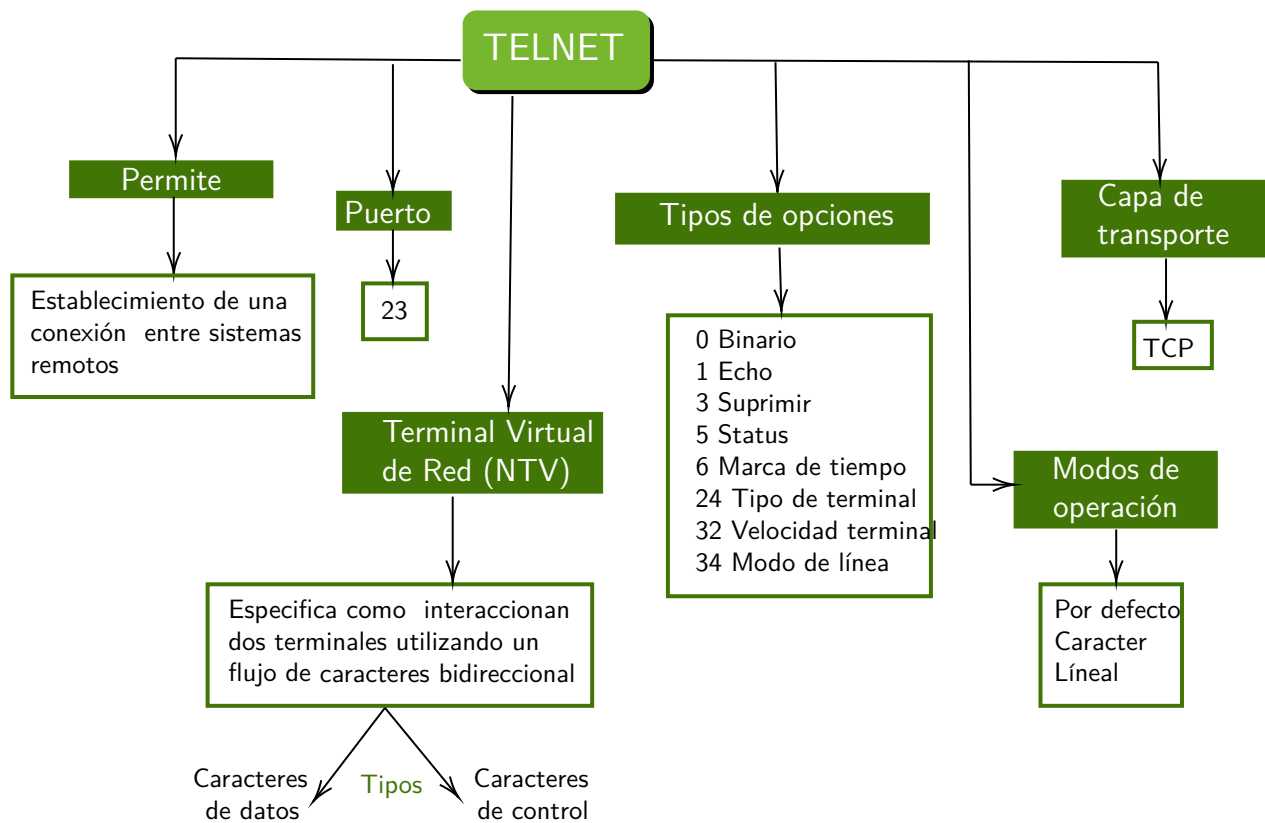
## 3.9 Comandos de usuario disponibles

El usuario normal no usa los comandos TELNET. Por lo general, el sistema operativo (UNIX, por ejemplo) define una interfaz con comandos fáciles de usar. Un ejemplo de este conjunto de comandos se puede encontrar en la tabla siguiente. Se tiene que tomar en cuenta que la interfaz es responsable de traducir los comandos fáciles de usar a los definidos previamente, comandos en el protocolo.

## 3.10 Mapa conceptual

**Tabla 7:** Ejemplos de comandos de interfaz

Comando	Significado.
open	Conectarse a una computadora remota.
close	Cerrar la conexión.
display	Mostrar los parámetros de funcionamiento.
mode	Cambiar a modo de línea o carácter.
set	Establecer los parámetros de funcionamiento.
status	Mostrar la información de estado.
send	Enviar caracteres especiales.
quit	Salir de TELNET.



## 4 FTP

### 4.1 Función principal del protocolo

Su función radica en permitir a los sistemas principales transferir datos entre sistemas principales diferentes, así como archivos entre dos sistemas principales externos de forma indirecta.

### 4.2 Capa de transporte utilizada

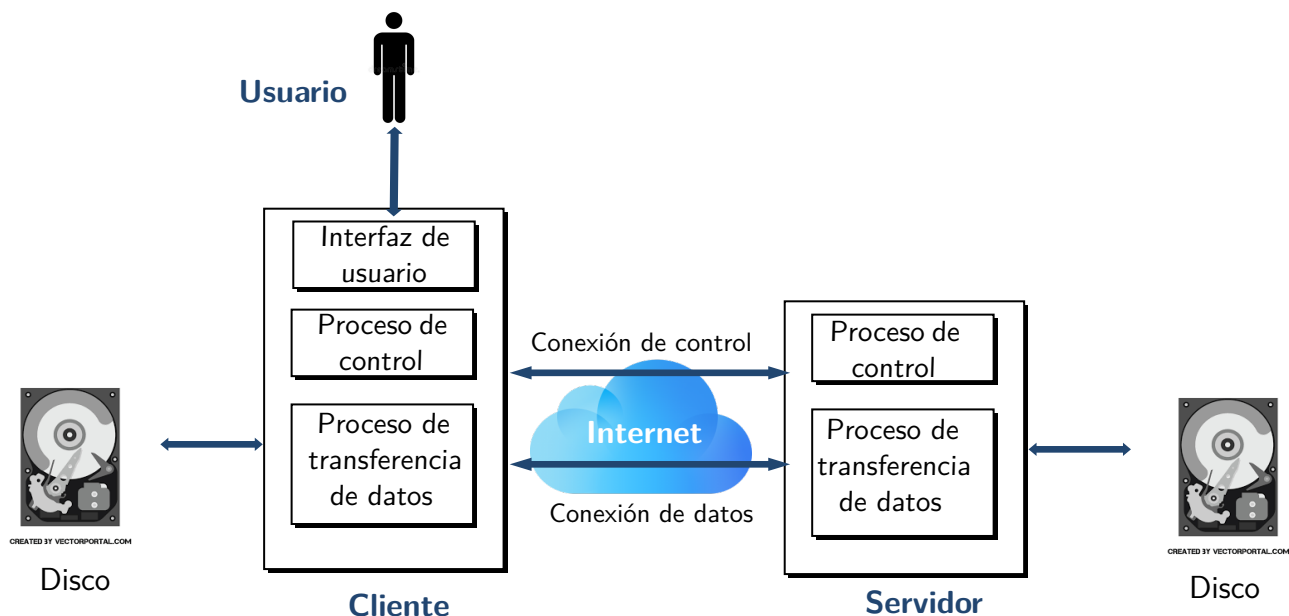
FTP utiliza los servicios de TCP para enviar los archivos y utiliza una conexión Telnet para transferir mandatos y respuestas.

### 4.3 Puertos utilizados para establecer una sesión FTP

FTP Necesita dos conexiones TCP. El puerto bien conocido 21 para la conexión de control y puerto bien conocido 20 para la conexión de datos.

### 4.4 Modelo básico FTP

El cliente tiene tres componentes: interfaz de usuario, proceso de control del cliente y proceso de transferencia de datos del cliente. El servidor tiene dos componentes: el proceso de control del servidor y el proceso de transferencia de datos del servidor. La conexión de control permanece conectada durante toda la sesión FTP interactiva.



**Figura 11:** Modelo básico FTP

Cuando un usuario inicia una sesión FTP, se abre la conexión de control. Mientras la conexión de control está abierta, la conexión de datos puede abrirse y cerrarse varias veces si se transfieren varios archivos.



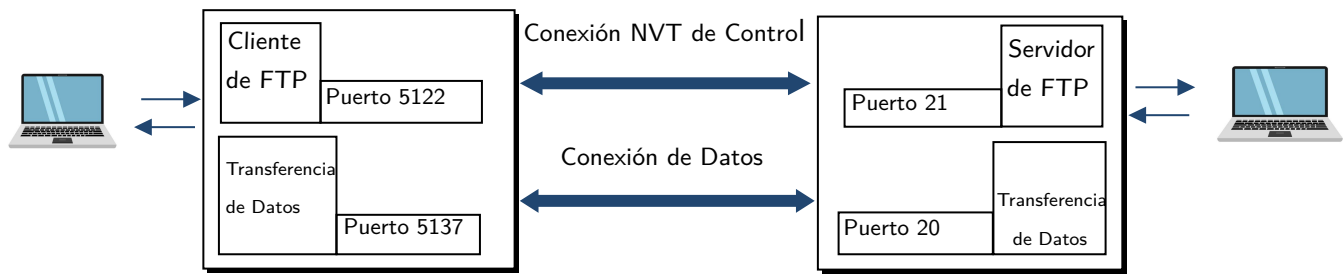


Figura 12: Diagrama del servicio FTP

## 4.5 Tipos de conexiones existentes

Cuando una aplicación cliente FTP inicia una conexión a un servidor FTP, abre el puerto 21 en el servidor conocido como el puerto de comandos. Se utiliza este puerto para arrojar todos los comandos al servidor. FTP admite dos modos de conexión del cliente. Estos modos se denominan Activo (o Estándar, o PORT, debido a que el cliente envía comandos tipo PORT al servidor por el canal de control al establecer la conexión) y Pasivo (o PASV, porque en este caso envía comandos tipo PASV). Tanto en el modo Activo como en el modo Pasivo, el cliente establece una conexión con el servidor.

Las dos conexiones FTP, control y datos, utilizan diferentes estrategias y diferentes números de puerto.

### Conexión de control

Pasos:

1. El servidor emite una apertura pasiva en el puerto bien conocido 21 y espera un cliente.
2. El cliente utiliza un puerto efímero y emite una apertura activa.

La conexión permanece abierta durante todo el proceso. El tipo de servicio, utilizado por el protocolo IP es minimizar el retardo porque se trata de una conexión interactiva entre un usuario (humano) y un servidor. El usuario teclea comandos y espera recibir respuestas sin retraso significativo.

### Conexión de datos

La conexión de datos utiliza puerto bien conocido 20 del servidor. Pasos: [7]

1. El cliente, no el servidor, emite una apertura pasiva utilizando un puerto efímero. Esto debe hacerlo el cliente porque es él quien emite los comandos para transferir archivos.
2. El cliente envía este número de puerto al servidor utilizando el comando PORT.
3. El servidor recibe el número de puerto y emite una apertura activa utilizando el puerto bien conocido 20 y el número de puerto efímero recibido.

## 4.6 Componentes de un cliente FTP

- **Interfaz de usuario:** conjunto de comandos de “alto nivel” que el usuario puede memorizar más fácilmente que los comandos FTP que se envían entre cliente y servidor.

- **Cliente PI:** El intérprete de protocolo de usuario inicia el control de la conexión a través del puerto 21 con el servidor FTP, envía los comandos FTP una vez codificados por la interfaz de usuario y los envía al intérprete de protocolo del servidor, y controla el proceso de transferencia de los archivos (DTP).
- **Cliente DTP:** El proceso de transferencia de datos “escucha” el puerto de datos (20) aceptando conexiones para la transferencia de ficheros.

## 4.7 Componentes de un servidor FTP

- **Servidor PI (Protocol Interpreter):** El intérprete de protocolo del servidor “escucha” en el puerto 21, los comandos que le envía el intérprete de protocolo del cliente y controla el proceso de transferencia de datos del servidor.
- **Servidor DTP (Data Transfer Protocol):** El protocolo de transferencia de datos del servidor se utiliza para transmitir los datos entre el servidor y el protocolo de transferencia de datos del cliente. Puede estar en modo “pasivo” a la escucha de conexiones en el puerto 20 de datos.

## 4.8 Problema de la heterogeneidad

El cliente y el servidor FTP, que se ejecutan en distintas computadoras, deben comunicarse entre sí, sin embargo, estos pueden utilizar diferentes sistemas operativos, diferentes conjuntos de caracteres, estructuras de archivo y formatos de archivo diferentes. FTP debe hacer compatible esta heterogeneidad. FTP tiene dos enfoques diferentes, uno para la conexión de control y otro para la de conexión de datos.

### Comunicación a través de la conexión de control

FTP utiliza el mismo enfoque que TELNET o SMTP para comunicarse a través de la conexión de control

- Utiliza el juego de caracteres ASCII NV
- Comunicación mediante comandos y respuestas.
- Envía un solo comando (o respuesta) a la vez.
- Cada comando o respuesta es sólo una línea corta

### Comunicación a través de la conexión de datos

El cliente debe definir el tipo de fichero a transferir, la estructura de los datos y el modo de transmisión. Antes de enviar el fichero a través de la conexión de datos, preparamos la transmisión a través de la conexión de control. la conexión de control. [8]

## 4.9 Atributos de comunicación

### Tipo de Archivo

FTP puede transferir uno de los siguientes tipos de archivos a través de la conexión de datos:

## Archivo ASCII

- **Archivo ASCII:** Este es el formato por defecto para transferir archivos de texto. Cada carácter se codifica utilizando NVT ASCII.
- **Archivo EBDIC** (para ambos extremos)
- **Archivo de Imagen:** Este es el formato por defecto para transferir archivos binarios.

## Estructura de datos

Para transferir un archivo FTP puede utilizar:

- **Estructura de archivos (predeterminada) :** El archivo no tiene estructura. Es un flujo continuo de bytes.
- **Estructura del registro:** El archivo se divide en registros. Solo para archivos de texto.
- **Estructura de la página:** El archivo está dividido en páginas, y cada página tiene un número y encabezado. Las páginas se pueden almacenar y acceder de forma aleatoria o secuencialmente.

## Modo de transmisión

- **Modo de transmisión (por defecto) :** Los datos se entregan de FTP a TCP como un flujo continuo de bytes. TCP es responsable de dividir los datos en segmentos de tamaño apropiado. Para indicar el final:
  - *Para estructura de archivo:* no se necesita un archivo final, el fin del archivo es el cierre de la conexión de datos por parte del transmisor
  - *Para estructura de registro:* cada registro tendrá un carácter de fin de registro (EOR) de 1 byte y el final del archivo tendrá un carácter de 1 byte de fin de archivo (EOF).
- **Modo bloque:** cada bloque está precedido por un encabezado de 3 bytes. El primer byte se denomina descriptor de bloque; los dos bytes siguientes definen el tamaño del bloque en bytes.
- **Modo comprimido:** Si el archivo es grande, los datos se pueden comprimir, el método de compresión normalmente utilizado es la codificación de longitud de ejecución.

FTP mantiene el transporte seguro pasando contraseñas de usuario y cuenta al sistema principal externo. Aunque FTP está principalmente diseñado para que lo utilicen las aplicaciones, también permite sesiones interactivas orientadas al usuario. [9]

## 4.10 Tipos de comando y su uso

Los comandos, que se envían desde el proceso de control del cliente FTP, tienen la forma de mayúscula ASCII, que puede ir seguida o no de un argumento. Se puede dividir los comandos en seis grupos: comandos de acceso, comandos de administración de archivos, comandos de formateo de datos, comandos de definición de puertos, comandos de transferencia de archivos y comandos misceláneos.

## Comandos de acceso

Permiten al usuario acceder al sistema remoto.

## Comandos de gestión de archivos

Permiten al usuario acceder al sistema de archivos, en la computadora remota. Permiten navegar por el directorio estructura, crear nuevos directorios, eliminar archivos, etc.

## Comandos de formateo de datos

Permiten al usuario definir la estructura de datos, el tipo de archivo y el modo de transmisión. El formato definido es luego utilizado por el archivo.

## Comandos de definición de puertos

Definen el número de puerto para la conexión de datos en el sitio del cliente. Hay dos métodos : usando el comando PORT (el cliente elige el puerto )y usando el comando PARSV (el servidor elige el puerto).

## Comandos de transferencia de archivos

Permiten que el usuario transfiera archivos.

## Comandos misceláneos

Entregan información al usuario FTP en el sitio del cliente.

Los comandos más utilizados podrían llegar a ser:

**Tabla 8:** Comandos FTP

<b><i>ftp</i></b>	Accede al intérprete de comandos ftp.
<b><i>ftp sistema remoto</i></b>	Establece una conexión ftp a un sistema remoto.
<b><i>delete, mdelete</i></b>	Elimina un archivo o varios, del directorio de trabajo remoto.
<b><i>open</i></b>	Inicia sesión en el sistema remoto desde el intérprete de comandos.
<b><i>close</i></b>	Cierra la sesión del sistema remoto y vuelve al intérprete de comandos.
<b><i>put, input</i></b>	Copia un archivo o varios, en el directorio de trabajo local al directorio de trabajo remoto.
<b><i>bye</i></b>	Sal del intérprete de comandos ftp.
<b><i>get, mget</i></b>	Copia un archivo o varios, del directorio de trabajo remoto al directorio de trabajo local.
<b><i>help</i></b>	Muestra todos los comandos ftp o, si se proporciona un nombre de comando, se describe brevemente lo que hace el comando.
<b><i>rmdir</i></b>	Elimina un directorio en el sistema remoto.
<b><i>reset</i></b>	Vuelve sincronizar la secuenciación de respuesta de comando con el servidor ftp remoto.
<b><i>mkdir</i></b>	Crea un directorio en el sistema remoto.
<b><i>ls</i></b>	Muestra los contenidos del directorio de trabajo remoto.
<b><i>lcd</i></b>	Cambia el directorio de trabajo local.
<b><i>pwd</i></b>	Muestra el nombre del directorio de trabajo remoto.
<b><i>cd</i></b>	Cambia el directorio de trabajo remoto.

## 4.11 Tipos de códigos de respuesta

### Respuesta preliminar positiva

Estos códigos de estado indican que una acción se ha iniciado correctamente.

- **110:** respuesta del marcador de reinicio.
- **120:** servicio listo en n minutos.
- **125:** conexión de datos ya abierta; inicio de transferencia.
- **150:** el estado del archivo está bien; a punto de abrir la conexión de datos.

### Respuesta de finalización positiva

Una acción se ha completado correctamente. El cliente puede ejecutar un nuevo comando.

- **200:** comando correcto.
- **202:** comando no implementado, superfluo en este sitio.
- **211:** Estado del sistema o ayuda del sistema para responder.
- **212:** Estado del directorio.
- **213:** Estado del archivo.

### Respuesta intermedia positiva

El comando se ha realizado correctamente, pero el servidor necesita información adicional del cliente.

- **331:** nombre de usuario correcto, necesita contraseña.
- **332:** necesita cuenta para iniciar sesión.
- **334:** Mecanismo de seguridad solicitado correcto.
- **335:** los datos de seguridad son aceptables. Se necesitan más datos para completar el Intercambio de datos de seguridad.
- **336:** Nombre de usuario correcto, necesita contraseña. [10]

### Respuesta de finalización negativa transitoria

El comando no se ha realizado correctamente, pero el error es temporal. Si el cliente vuelve a instar al comando, puede que se haga correctamente.

- **421:** servicio no disponible, conexión de control de cierre. Puede ser una respuesta a cualquier comando si el servicio sabe que debe apagarse.
- **425:** no se puede abrir la conexión de datos.
- **426:** conexión cerrada; transfer aborted.
- **431:** necesita algún recurso no disponible para procesar la seguridad.

## 4.12 Transferencia de archivos

La transferencia de archivos se produce a través de la conexión de datos bajo el control de los comandos enviados a través de la conexión de control. Puede ocurrir que:

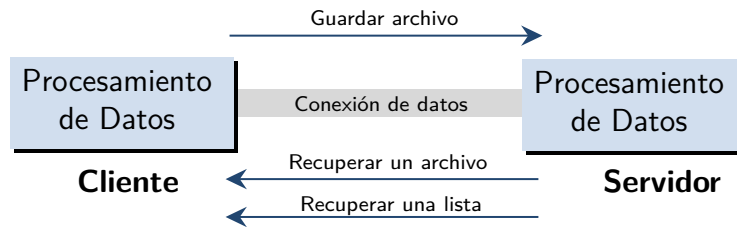
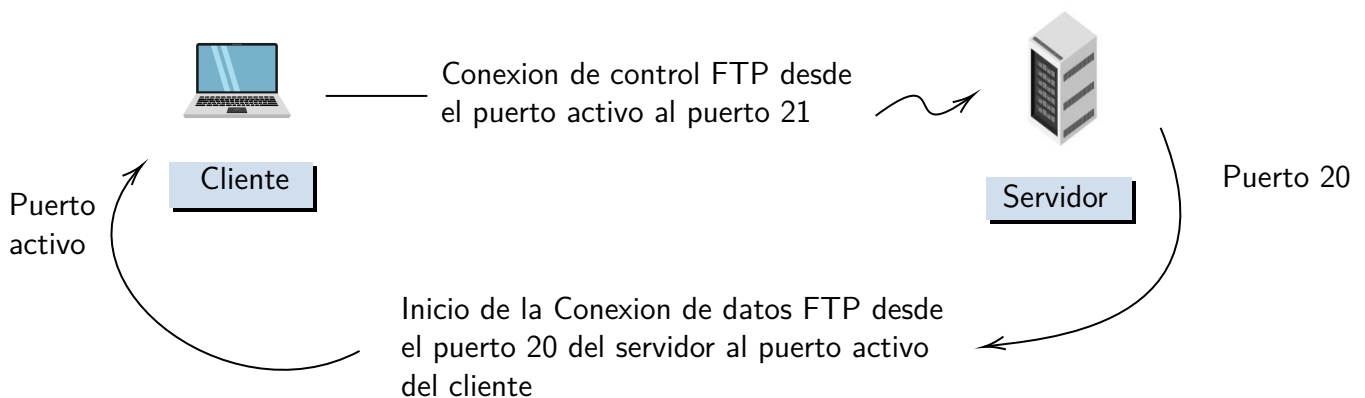


Figura 13

- **RETR** va a copiar un fichero del servidor al cliente (descarga), denominado: recuperar un archivo.
- **STOR** Copiar un fichero del cliente al servidor (upload), denominado: almacenar un archivo
- **LIST** Una lista de nombres de directorios o archivos debe enviarse del servidor al cliente.

### FTP Activo



### FTP Pasivo

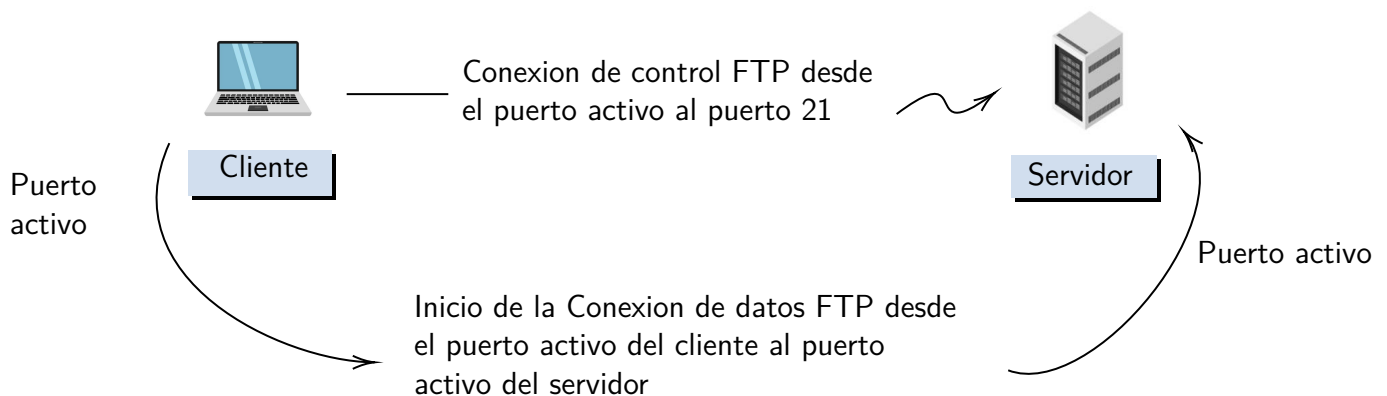


Figura 14: Diagrama de transferencia de un archivo

## 4.13 Mapa Conceptual

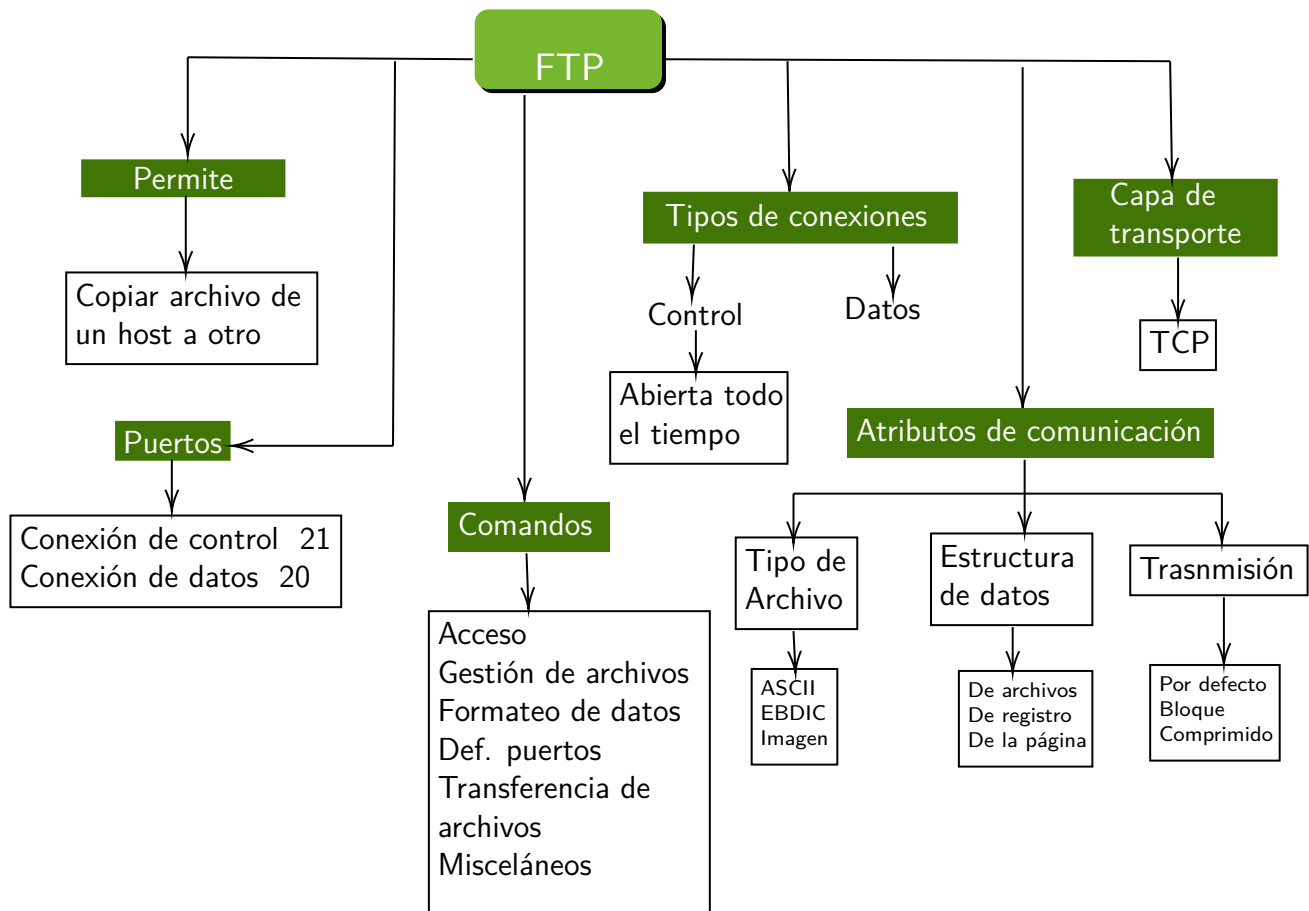


Figura 15



# 5 HTTP

## 5.1 Función principal del protocolo

La función de HTTP es proporcionar acceso a los sistemas de archivos mediante los protocolos HTTP y HTTPS (WebDAV) y mediante el sistema distribuido de creación y control de versiones web de la extensión HTTP (WebDAV). Esto permite que los clientes accedan a sistemas de archivos compartidos mediante un explorador web o un sistema de archivos local si el software del cliente lo admite.

## 5.2 Capa de transporte utilizada

HTTP utiliza una conexión TCP para transferir archivos. Las transacciones HTTP están formadas por mensajes de solicitud y respuesta.

## 5.3 Puertos utilizados para establecer una sesión HTTP

El puerto predeterminado de HTTP es el 80 a través del protocolo TCP y el puerto 443 a través del protocolo SSL/TLS.

## 5.4 Significado y campos de un URL (Localizador Uniforme de Recursos)

El localizador uniforme de recursos (URL) es un localizador estándar para especificar cualquier tipo de información en Internet. Un URL no es más que una dirección que es dada a un recurso único en la Web. En teoría, cada URL válida apunta a un único recurso. Dichos recursos pueden ser páginas HTML, documentos CSS, imágenes, etc. El URL define cuatro partes: protocolo, ordenador anfitrión, puerto y ruta. [12]



Figura 16: URL

- **Protocolo:** El protocolo es un programa de aplicación cliente-servidor utilizado para recuperar el documento. Muchos protocolos diferentes pueden recuperar un documento; entre ellos se encuentran Gophers, FTP, HTTP, News y TELNET. El más común hoy en día es HTTP.
- **Host:** Nombre de dominio el cual indica qué servidor web se solicita. Aunque, alternativamente, es posible usar directamente una dirección IP, pero debido a que es menos conveniente, no se usa con frecuencia en la Web (Es por ello que se recurre al DNS).
- **Puerto:** Indica la "puerta", técnica utilizada para acceder a los recursos en el servidor web. Por lo general, se omite si el servidor web utiliza los puertos estándar del protocolo HTTP (80 para HTTP y 443 para HTTPS) para otorgar acceso a sus recursos.
- **Ruta:** Sigue la ruta al recurso en el servidor web. [12]

## 5.5 Tipos de mensajes y sus campos

Los clientes y los servidores se comunican intercambiando mensajes individuales (en contraposición a las comunicaciones que utilizan flujos continuos de datos). Los mensajes que envía el cliente, normalmente un navegador Web, se llaman peticiones, y los mensajes enviados por el servidor se llaman respuestas.

Entonces, existen dos tipos de mensajes HTTP: **peticiones y respuestas**, cada uno sigue su propio formato.

### Respuestas

- La versión del protocolo HTTP que están usando.
- Un código de estado, indicando si la petición ha sido exitosa, o no, y debido a que.
- Un mensaje de estado, una breve descripción del código de estado.
- Cabeceras HTTP, como las de las peticiones.
- Opcionalmente, el recurso que se ha pedido.

### Peticiones

- Un método HTTP: normalmente un verbo (como get o post) o un nombre como options o head que defina la operación del usuario
- La dirección del recurso pedido: la URL del recurso, sin los elementos obvios por el contexto (sin el protocolo http) ni el dominio o el puerto
- La versión de protocolo
- Cabeceras opcionales que pueden aportar información a los servidores
- Cuerpo del mensaje, en algún método que enviar información al servidor

## 5.6 Métodos

HTTP también define un conjunto de métodos de petición para indicar la acción que se desea realizar para un recurso determinado. Aunque estos también pueden ser sustantivos, estos métodos de solicitud a veces son llamados HTTP verbs.

**GET:** solicita una representación de un recurso específico. Las peticiones que usan el método GET sólo deben recuperar datos.

**HEAD:** pide una respuesta idéntica a la de una petición GET, pero sin el cuerpo de la respuesta.

**POST:** se utiliza para enviar una entidad a un recurso en específico, causando a menudo un cambio en el estado o efectos secundarios en el servidor.

**PUT:** reemplaza todas las representaciones actuales del recurso de destino con la carga útil de la petición.

**DELETE:** borra un recurso en específico.

**CONNECT:** establece un túnel hacia el servidor identificado por el recurso.[\[13\]](#)

## 5.7 Códigos de respuesta o estado

Los códigos de estado de respuesta HTTP indican si se ha completado satisfactoriamente una solicitud HTTP específica. Las respuestas se agrupan en cinco clases:

1. Respuestas informativas (100–199)
2. Respuestas satisfactorias (200–299)
3. Redirecciones (300–399): Significan mensajes que mencionan el cambio de recurso en la URI, o para redirigir al cliente a un nuevo recurso solicitado a una nueva dirección, que se debe tener acceso desde un proxy, etc.
4. Errores de los clientes (400–499)
5. Errores de los servidores (500–599)

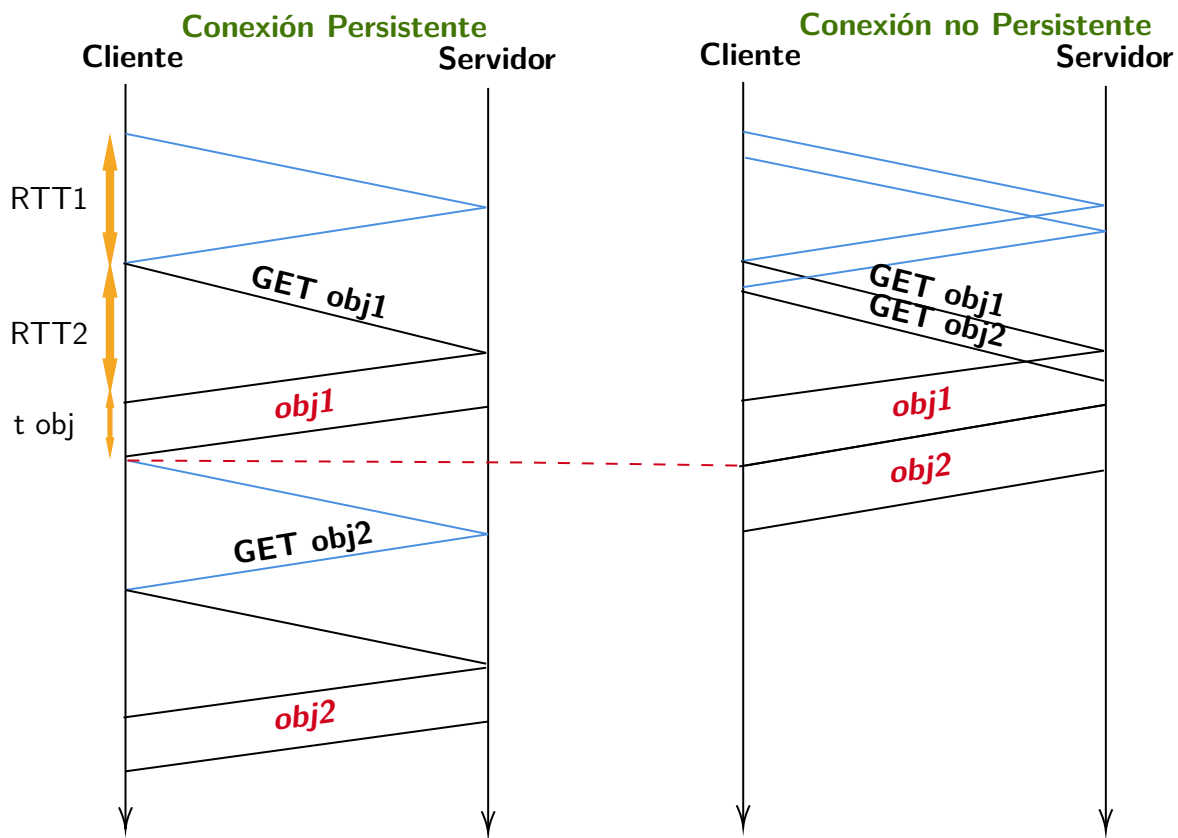
## 5.8 Diagramas de secuencia para una conexión persistente y una no persistente

### Conexiones no persistentes.

Se denominan conexiones breves y son aquellas que duran unos pocos momentos además de no utilizar el protocolo TCP como capa de transporte. Se utilizaban en el primer protocolo de HTTP debido a que se generaba una conexión para cada mensaje a utilizar.

### Conexiones persistentes.

Son aquellas que permanecen abiertas por un periodo, y pueden ser reutilizadas por varias peticiones de datos, ahorrando así la necesidad de efectuar nuevas sincronizaciones a nivel de TCP. [\[14\]](#)



**Figura 17:** Diagramas de secuencia de conexión persistente y no persistente

## 5.9 Uso de cookies

Una cookie HTTP, cookie web o cookie de navegador es una pequeña pieza de datos que un servidor envía al navegador web del usuario. El navegador guarda estos datos y los envía de regreso junto con la nueva petición al mismo servidor.

[15] Las cookies se utilizan principalmente con tres propósitos:

- Gestión de Sesiones: Inicios de sesión, carritos de compras, puntajes de juegos o cualquier otra cosa que el servidor deba recordar .
- Personalización: Preferencias de usuario, temas y otras configuraciones .
- Rastreo: Guardar y analizar el comportamiento del usuario. [16]

## 5.10 Mapa Conceptual

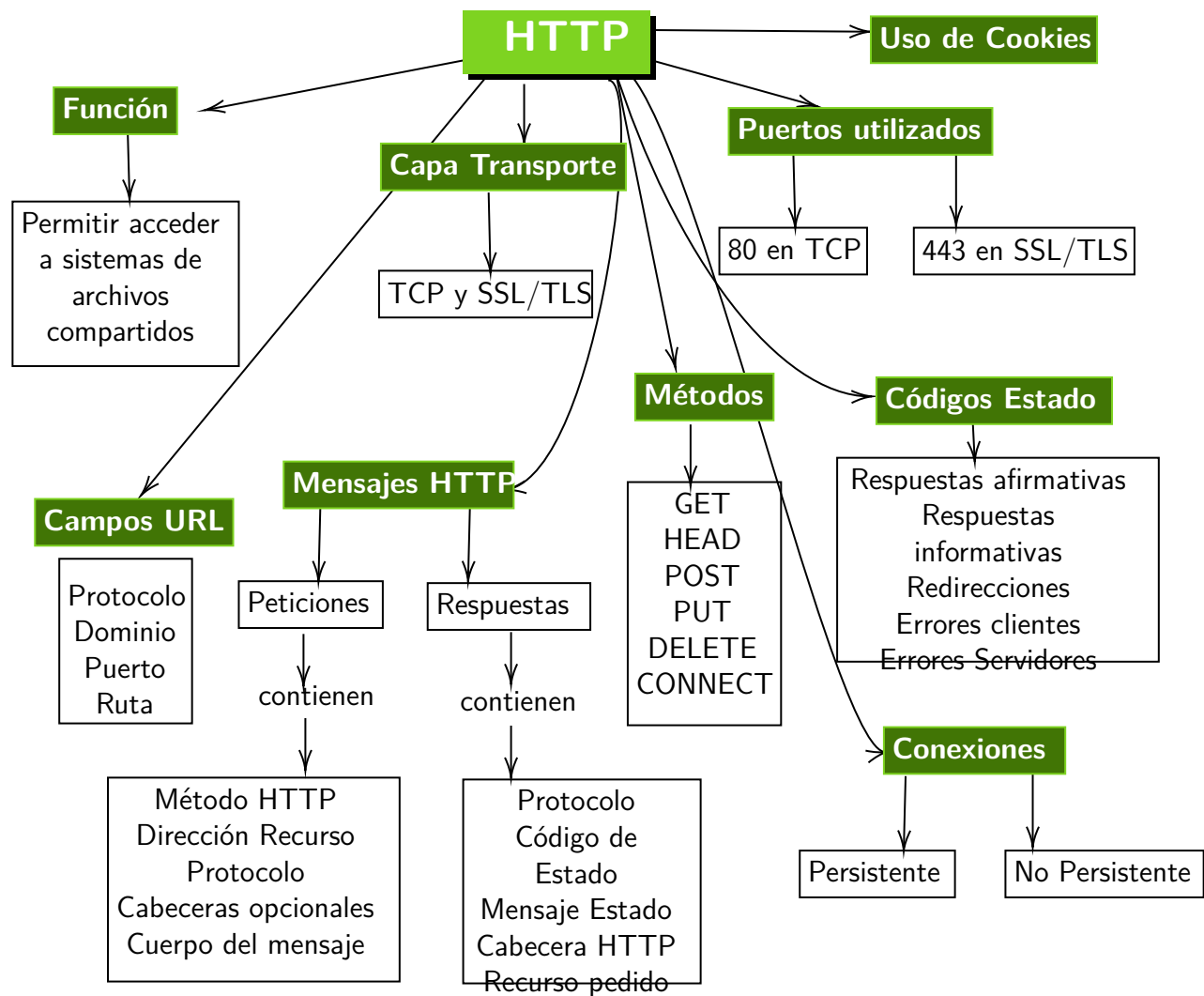


Figura 18

## 6 SMTP,POP y IMAP4

### 6.1 Función principal de cada protocolo

SMTP es un servidor de salida, encargado de enviar los correos, distribuirlos, y entregarlos a su destino mientras que IMAP Y POP3 son servidores de entrada, se encargan de almacenar y organizar los correos, una vez recibidos.

### 6.2 Capa de transporte utilizada por cada uno de los protocolos

SMTP, POP e IMAP4 ocupan el protocolo TCP de la capa de transporte.

### 6.3 Puertos utilizados para establecer una sesión SMTP

Mientras que el servidor SMTP utiliza el conocido puerto 25, el POP3 lo hace a través del puerto 110 y el IMAP hace lo correspondiente con el 143.

### 6.4 Diagrama de secuencia para el establecimiento de sesión

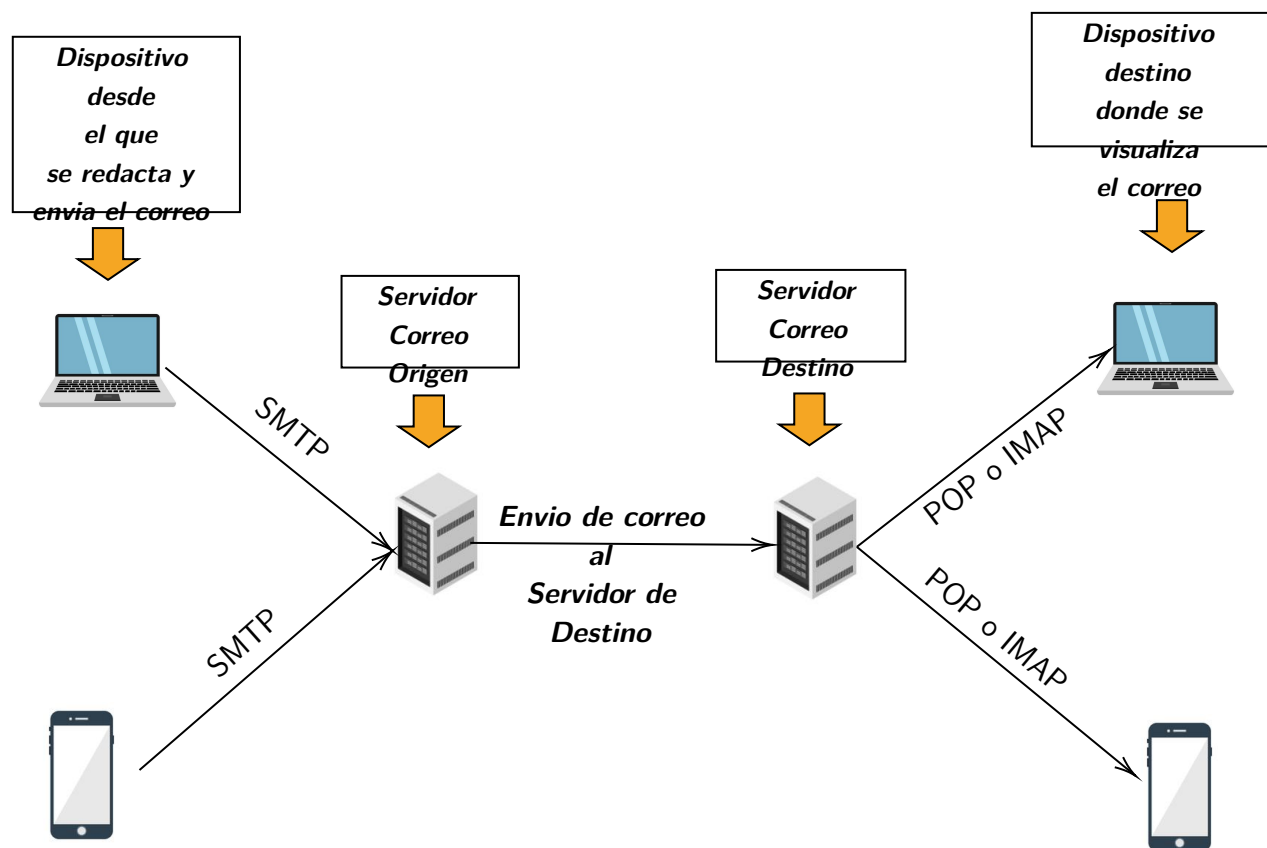


Figura 19

## 6.5 Función del Agente de Usuario (UA, User Agent)

Agente de usuario de correo es el cliente de correo electrónico propiamente dicho. Le va a permitir al usuario leer mensajes del servidor de correo entrante y escribir mensajes a través del servidor de correo saliente. Ejemplos de agentes MUA son: Pine, Evolution, Outlook, Thunderbird, etc. Sus características más importantes son:

- Dispone de una funcionalidad MIME para leer o escribir mensajes no ASCII, para incluir imágenes o ficheros adjuntos.
- Utiliza los formatos MBOX o MAILDIR para almacenar los mensajes en modo local.

## 6.6 Función del Agente de transferencia de mensajes (MTA, Message Transfer Agent,)

El agente de transferencia de correo se encarga de la transferencia de mensajes de correo electrónico entre las máquinas mediante la utilización del protocolo SMTP. Un mensaje desde el origen hasta su destino puede pasar por varios MTA. Utiliza el puerto 25 y el puerto 587 (el primero para enviar correos al exterior y el segundo para los usuarios locales cuando está bloqueada la salida al exterior).

### Función de los Agentes de acceso a mensajes (MAA, Message Access Agent)

Su función radica en encargarse del acceso al correo almacenado. El protocolo más usado es POP3 (Post-Office Protocol versión 3). Se encarga de hacer accesible los buzones a equipos remotos.

### Ventajas y desventajas de POP3 e IMAP4

#### Ventajas

##### POP3:

- Si tu cuenta se configura como POP3, los correos serán descargados directamente desde el servidor a tu equipo, por lo que no ocuparán espacio en tu hosting.
- Permite consultar los correos siempre desde tu equipo, aunque no tengas conexión a Internet.

##### IMAP4:

- Puede consultar los correos desde diferentes ubicaciones y / o gestores de correo.
- Consulta tu cuenta desde casa, en tu móvil, tableta, a través de Webmail, etc.
- Dispone de una copia de seguridad de tus correos, que puedes recuperar en caso de pérdida.
- Sincroniza todas las carpetas que tengas en tu cuenta de correo con los demás dispositivos incluyendo la carpeta de correos enviados.

## Desventajas

### POP3:

No dispondrás de copia de los correos en el servidor. Tampoco podrás visualizarlos desde diferentes dispositivos, a menos que habilites en tu gestor de correo la opción Mantener copia de los mensajes en el servidor. Con esta opción mantendremos una copia, pero solo de la carpeta de entrada. No se sincronizarán las demás carpetas que tengas creadas en el servidor, ya que se consideran como carpetas IMAP.

### IMAP4:

Si configuras tu cuenta como IMAP, tus emails serán visualizados desde tu gestor de correo, pero físicamente estarán almacenados en el servidor. Esta opción consumirá espacio en tu hosting.[17]

## Formato de un email

Un correo electrónico se compone de un encabezado, un cuerpo y un sobre .

**Encabezado:** Contiene instrucciones de enrutamiento e información acerca del mensaje. Algunos ejemplos son la dirección del remitente, o la dirección del destinatario.

**Cuerpo:** Contiene el texto del propio mensaje .

**Sobre:** Contiene la información de enrutamiento real que se comunica entre el cliente de correo electrónico y el servidor de correo durante la sesión SMTP. Esta información de sobre de correo electrónico es análoga a la información en un sobre postal.

La estructura de un email se puede observar en la siguiente imagen:

## 6.7 Formato de las direcciones de correo

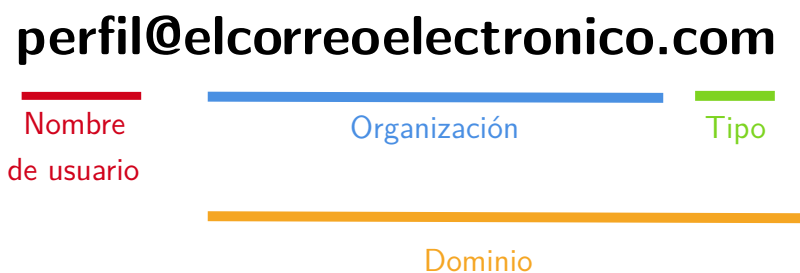


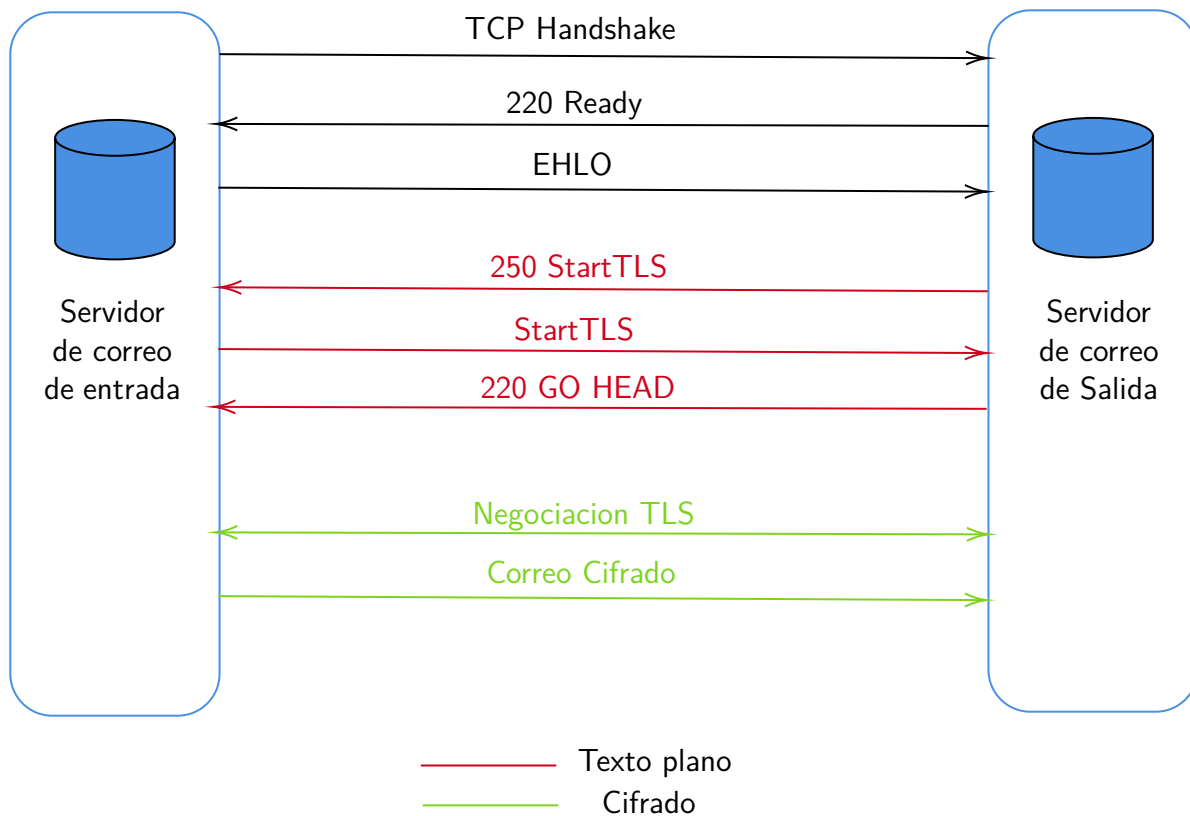
Figura 20: Formato de un correo

## Comandos y respuestas utilizadas por SMTP

Para establecer la conexión entre los protocolos, SMTP maneja los comandos: [18] EHLO: Permite al servidor declarar su aceptación de comandos, ESMTP (Extended Simple Mail Transfer Protocol). MAIL FROM: Emisor del mensaje. RCPT TO: Receptor(es) del mensaje. DATA: Lo envía el cliente para indicar que inicia el envío del contenido del mensaje. QUIT: Finaliza la sesión. [19]



**Diagrama de secuencia que represente las fases de transferencia de un email que muestre el intercambio de los comandos utilizados**



**Figura 21**

## 6.8 Mapa Conceptual

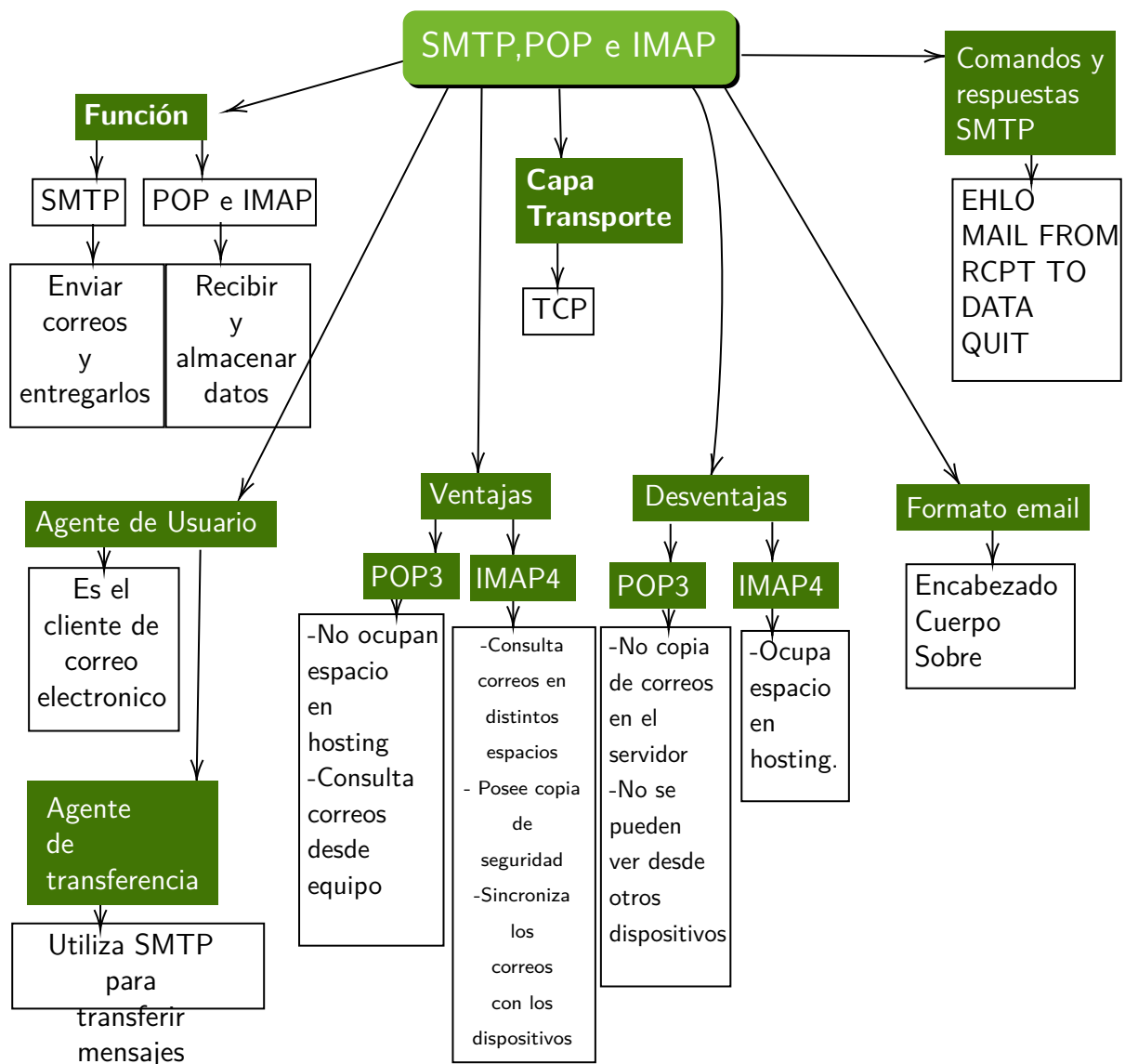


Figura 22

# Bibliografía

- [1] "3.1.- mensajes dhcp." [Online]. Available: [https://ikastaroak.birt.eus/edu/argitalpen/backupa/20200331/1920k/es/ASIR/SRI/SRI01/es\\_ASIR\\_SRI01.Contenidos/website\\_31.mensajes\\_dhcp.html](https://ikastaroak.birt.eus/edu/argitalpen/backupa/20200331/1920k/es/ASIR/SRI/SRI01/es_ASIR_SRI01.Contenidos/website_31.mensajes_dhcp.html)
- [2] B. A. Forouzan, *TCP/IP protocol suite*. McGraw Education (India) Private Limited, 2017.
- [3] "DNS - Domain Name System - javatpoint." [Online]. Available: <https://www.javatpoint.com/computer-network-dns>
- [4] J. Jung, E. Sit, H. Balakrishnan, and R. Morris, "Dns performance and the effectiveness of caching," *ACM SIGCOMM Computer Communication Review*, vol. 32, 08 2002.
- [5] J. Thomas, "What is telnet," OmniSecu. [Online]. Available: <https://www.omniseu.com/about.php>
- [6] , "Tcp - transmission control protocol (client uses telnet to log into server)," PDF, may 2012. [Online]. Available: <https://www.eventhelix.com/networking/Telnet.pdf>
- [7] B. E., "Servidores de ficheros mediante ftp y tftp." PDF. [Online]. Available: <http://informatica.uv.es/it3guia/AGR/apuntes/teoria/documentos/FTP.pdf>
- [8] I. Corporation, "Protocolo de transferencia de archivos (file transfer protocol)." [Online]. Available: <https://www.ibm.com/docs/es/aix/7.1?topic=protocols-file-transfer-protocol>
- [9] , *Red Hat Enterprise Linux: Manual de Referencia*. Capítulo 15.
- [10] , "Códigos de estado ftp en iis 7.0 y versiones anteriores." 2022. [Online]. Available: <https://docs.microsoft.com/es-es/troubleshoot/developer/webapps/iis/ftp-service-svchost-inetinfo/ftp-status-codes-iis-7-and-later-versions>
- [11] "Inicio de sesión en un sistema remoto (ftp)." [Online]. Available: [https://docs.oracle.com/cd/E24842\\_01/html/E22524/remotehowtoaccess-14.html](https://docs.oracle.com/cd/E24842_01/html/E22524/remotehowtoaccess-14.html)
- [12] Oracle, "Protocolo de transferencia de hipertexto (http)." [Online]. Available: [https://docs.oracle.com/cd/E55837\\_01/html/E54251/makehtml-id-33.html](https://docs.oracle.com/cd/E55837_01/html/E54251/makehtml-id-33.html)
- [13] , "Generalidades del protocolo http." [Online]. Available: [https://developer.mozilla.org/es/docs/Web/HTTP/Overview#caracter%C3%ADsticas\\_clave\\_del\\_protocolo\\_http](https://developer.mozilla.org/es/docs/Web/HTTP/Overview#caracter%C3%ADsticas_clave_del_protocolo_http)
- [14] , "¿qué es una url?" [Online]. Available: [https://developer.mozilla.org/es/docs/Learn/Common\\_questions/What\\_is\\_a\\_URL](https://developer.mozilla.org/es/docs/Learn/Common_questions/What_is_a_URL)
- [15] , "Códigos de estado de respuesta http." [Online]. Available: <https://developer.mozilla.org/es/docs/Web/HTTP/Status>
- [16] , "Metodos de peticion http." [Online]. Available: <https://developer.mozilla.org/es/docs/Web/HTTP/MethodsL>
- [17] "Formato de correo electrónico y amazon ses." 2020. [Online]. Available: [https://docs.aws.amazon.com/es\\_es/ses/latest/dg/send-email-concepts-email-format.html](https://docs.aws.amazon.com/es_es/ses/latest/dg/send-email-concepts-email-format.html)
- [18] B. M., "Email marketing: Cómo funcionan smtp, pop3 e imap." 2020. [Online]. Available: <https://blog.embluemail.com/como-funciona-smtp-pop3-e-imap/>

- [19] L. A., “Agentes del servicio de correo electrónico.” 2014. [Online]. Available: <https://www.profesordeinformatica.com/servicios/email/agentes#>