Departamento de
Automática y Computación
*Automatika eta*
*Konputazio Saila*

Campus de Arrosadía
*Arrosadiko Campusa*
31006 Pamplona - *Iruñea*
*Tfno. 948 169113, Fax. 948 168924*
*Email: ayc@unavarra.es*

# Práctica 7 – Protocolos de nivel de aplicación

## 1- Objetivos

En esta práctica estudiaremos diversos protocolos de la capa de aplicación: HTTP, FTP, Telnet y SMTP/POP3; los comandos existentes y problemas que se presentan. Capturaremos los paquetes transmitidos por la red con la herramienta Ethereal para luego extraer la información de la capa de aplicación y analizarla. Por último, nos familiarizaremos con la lectura de RFCs.

En esta segunda sesión veremos los protocolos TELNET y SMTP/POP3.

## 2- Avisos generales

Si quieren conservar cualquier fichero entre sesiones guárdenlo en una memoria USB, dado que no se asegura que los ficheros creados o modificados durante una sesión de prácticas se mantengan para la siguiente.

## 3- Protocolo Telnet

El protocolo Telnet es un protocolo de Internet estándar que permite conectar terminales y aplicaciones en Internet. El protocolo proporciona reglas básicas que permiten vincular a un cliente (PC) con un intérprete de comandos (del lado del servidor).

El protocolo Telnet se aplica en una conexión TCP para enviar datos en formato ASCII codificados en 8 bits, entre los cuales se encuentran secuencias de verificación Telnet. Por lo tanto, brinda un sistema de comunicación orientado bidireccional (semidúplex) codificado en 8 bits y fácil de implementar.

El protocolo Telnet se basa en tres conceptos básicos:

- El paradigma Terminal virtual de red (NVT);
- El principio de opciones negociadas;
- Las reglas de negociación.

Éste es un protocolo base, al que se le aplican otros protocolos del conjunto TCP/IP (FTP, SMTP, POP3, etc.). Las especificaciones Telnet no mencionan la autenticación porque Telnet se encuentra totalmente separado de las aplicaciones que lo utilizan (el protocolo FTP define una secuencia de autenticación sobre Telnet). Además, el protocolo Telnet no es un protocolo de transferencia de datos seguro, ya que los datos que transmite circulan en la red como texto sin codificar (de manera no cifrada). Cuando se utiliza el protocolo Telnet para conectar un host remoto a un equipo que funciona como servidor, a este protocolo se le asigna el puerto 23.

Excepto por las opciones asociadas y las reglas de negociación, las especificaciones del protocolo Telnet son básicas. La transmisión de datos a través de Telnet consiste sólo en transmitir bytes en el flujo TCP (el protocolo Telnet especifica que los datos deben agruparse de manera predeterminada —esto es, si ninguna opción especifica lo contrario— en un búfer antes de enviarse. Específicamente, esto significa que de manera predeterminada los datos se envían línea por línea). Cuando se transmite

Campus de Arrosadía
*Arrosadiko Campusa*
31006 Pamplona - *Iruñea*
*Tfno. 948 169113, Fax. 948 168924*
*Email: ayc@unavarra.es*

el byte 255, el byte siguiente debe interpretarse como un comando. Por lo tanto, el byte 255 se denomina IAC (Interpretar como comando). Los comandos se describen más adelante en este documento.

Las especificaciones básicas del protocolo Telnet se encuentran disponibles en la RFC (petición de comentarios) 854, mientras que las distintas opciones están descriptas en la RFC 855 hasta la RFC 861.

| RFC (peticiones de comentarios) relacionadas con Telnet | |
|---|---|
| RFC 854 | Especificaciones del protocolo Telnet |
| RFC 855 | Especificaciones de opciones de Telnet |
| RFC 856 | Transmisión binaria en Telnet |
| RFC 857 | Opción Eco de Telnet |
| RFC 858 | Opción de suprimir continuación en Telnet |
| RFC 859 | Opción Estado de Telnet |
| RFC 860 | Opción Marca de tiempo de Telnet |
| RFC 861 | Opción Lista extendida de opciones de Telnet |

**La noción de terminal virtual**

Cuando surgió Internet, la red (ARPANET) estaba compuesta de equipos cuyas configuraciones eran muy poco homogéneas (teclados, juegos de caracteres, resoluciones, longitud de las líneas visualizadas). Además, las sesiones de los terminales también tenían su propia manera de controlar el flujo de datos entrante/saliente.

Por lo tanto, en lugar de crear adaptadores para cada tipo de terminal, para que pudiera haber interoperabilidad entre estos sistemas, se decidió desarrollar una interfaz estándar denominada NVT (Terminal virtual de red). Así, se proporcionó una base de comunicación estándar, compuesta de:

- Caracteres ASCII de 7 bits, a los cuales se les agrega el código ASCII extendido;
- Tres caracteres de control;
- Cinco caracteres de control opcionales;
- Un juego de señales de control básicas.

Por lo tanto, el protocolo Telnet consiste en crear una abstracción del terminal que permita a cualquier host (cliente o servidor) comunicarse con otro host sin conocer sus características.

Campus de Arrosadía
*Arrosadiko Campusa*
31006 Pamplona - *Iruñea*
*Tfno. 948 169113, Fax. 948 168924*
*Email: ayc@unavarra.es*

## El principio de opciones negociadas

Las especificaciones del protocolo Telnet permiten tener en cuenta el hecho de que ciertos terminales ofrecen servicios adicionales, no definidos en las especificaciones básicas (pero de acuerdo con las especificaciones), para poder utilizar funciones avanzadas. Estas funcionalidades se reflejan como opciones. Por lo tanto, el protocolo Telnet ofrece un sistema de negociaciones de opciones que permite el uso de funciones avanzadas en forma de opciones, en ambos lados, al iniciar solicitudes para su autorización desde el sistema remoto.

Las opciones de Telnet afectan por separado cada dirección del canal de datos. Entonces, cada parte puede negociar las opciones, es decir, definir las opciones que:

- Desea usar (DO);
- Se niega a usar (DON'T);
- Desea que la otra parte utilice (WILL);
- Se niega a que la otra parte utilice (WON'T).

De esta manera, cada parte puede enviar una solicitud para utilizar una opción. La otra parte debe responder si acepta o no el uso de la opción. Cuando la solicitud se refiere a la desactivación de una opción, el destinatario de la solicitud no debe rechazarla para ser completamente compatible con el modelo NVT.

| Opciones negociadas de Telnet | | |
|---|---|---|
| Solicitud | Respuesta | Interpretación |
| DO | WILL | El remitente comienza utilizando la opción El remitente no debe utilizar la opción |
| | WON'T | El remitente no debe utilizar la opción |
| WILL | DO | El remitente comienza utilizando la opción, después de enviar *DO* |
| | DON'T | El remitente no debe utilizar la opción |
| DON'T | WON'T | El remitente indica que ha desactivado la opción |
| WON'T | DON'T | El remitente indica que el remitente debe desactivar la opción |

Existen 255 códigos de opción. De todas maneras, el protocolo Telnet proporciona un espacio de dirección que permite describir nuevas opciones. La RFC (petición de comentarios) 855 explica cómo documentar una nueva opción.

Campus de Arrosadía
*Arrosadiko Campusa*
31006 Pamplona - *Iruñea*
*Tfno. 948 169113, Fax. 948 168924*
*Email: ayc@unavarra.es*

### Las reglas de negociación

Las reglas de negociación para las opciones permiten evitar situaciones en las que una de las partes envía solicitudes de negociación de opciones a cada confirmación de la otra parte:

1. Las solicitudes sólo deben enviarse en el momento de un cambio de modo.
2. Cuando una de las partes recibe la solicitud de cambio de modo, sólo debe confirmar su recepción si todavía no se encuentra en el modo apropiado.
3. Sólo debe insertarse una solicitud en el flujo de datos en el lugar en el que surte efecto.

### Caracteres de control de salida

Los siguientes caracteres son comandos que permiten controlar la visualización del terminal virtual de red:

| Comandos de control para la visualización: | | | |
|---|---|---|---|
| Número; | Código | Nombre | Significado |
| 0 | NULL | Nulo | Este comando permite enviar datos al host remoto sin que se interpreten (en particular para indicar que el host local todavía esta en línea). |
| 1 | LF | Avance de línea | Este comando permite ubicar el cursor en la línea siguiente, en la misma posición horizontal. |
| 2 | CR | Retorno de carro | Este comando permite ubicar el cursor en el extremo izquierdo de la línea actual. |

Así, se define el comando CRLF, compuesto de dos comandos CR y LF uno después del otro (en cualquier orden). Esto permite ubicar el cursor en el extremo izquierdo de la línea siguiente.

### Caracteres de control opcionales

Los caracteres anteriores son los únicos (entre los 128 caracteres del código ASCII básico y los 128 caracteres del código ASCII extendido) que tienen un significado particular para el terminal virtual de red. Los siguientes caracteres pueden tener un significado en un terminal virtual de red, pero no se utilizan necesariamente.

| Comandos de control para la visualización | | | |
|---|---|---|---|
| Número | Código | Nombre | Significado |
| 7 | BEL | Campana | Este comando permite enviar una señal visual o sonora sin cambiar la posición del cursor. |
| 8 | BS | Retroceso | Este comando permite cambiar la posición del cursor a su posición anterior. |
| 9 | HT | Tabulación horizontal | Este comando permite que la posición del cursor pase a la siguiente tabulación a la derecha. |
| 11 | VT | Tabulación vertical | Este comando permite que la posición del cursor pase a la siguiente tabulación de la línea siguiente. |

Campus de Arrosadía
*Arrosadiko Campusa*
31006 Pamplona - *Iruñea*
*Tfno. 948 169113, Fax. 948 168924*
*Email: ayc@unavarra.es*

| | | | |
|---|---|---|---|
| 12 | FF | Avance de página | Este comando permite que la posición del cursor pase al final de la siguiente página mientras conserva su posición horizontal. |

### Caracteres de control de sesión

Los siguientes caracteres son comandos que permiten controlar la sesión Telnet. Para que puedan interpretarse como tal, estos comandos deben estar precedidos por el carácter de escape IAC (Interpretar como comando). Si estos bytes se transmiten sin estar precedidos por el carácter IAC, se procesarán como caracteres simples. Para transmitir el carácter IAC, este mismo debe estar precedido por un carácter de escape. En otras palabras, debe estar duplicado.

Los comandos relacionados con una negociación de opciones deben estar seguidos de un byte que especifique la opción. Estos comandos permiten interrumpir señales, eliminar información en el caché del terminal, etc.

| Caracteres de control de sesión | | | |
|---|---|---|---|
| Número | Código | Nombre | Significado |
| 240 | SE | | Fin de negociación de opciones |
| 241 | NOP | Sin operación | Este comando permite enviar datos al host remoto sin que se interpreten (en particular para indicar que el host local todavía esta en línea). |
| 242 | DM | Marca de datos | Permite vaciar todos los búferes entre el terminal virtual de red y el host remoto. Se relaciona con la pulsación del botón de sincronización (Synch) NVT y debe vincularse con una indicación de notificación urgente TCP. |
| 243 | BRK | Interrupción | Pausa de caracteres del terminal virtual. |
| 244 | IP | Interrumpir proceso | Este comando permite suspender, interrumpir o abandonar el proceso remoto. |
| 245 | AO | Abortar salida | Este comando permite suspender, interrumpir o abandonar la visualización del proceso remoto. |
| 246 | AYT | ¿Estás ahí? | Este comando permite controlar que el sistema remoto todavía esté "vivo". |
| 247 | EC | Borrar carácter | Este comando permite borrar el carácter anterior. |
| 248 | EL | Borrar línea | Este comando permite borrar la línea anterior. |
| 249 | GA | Adelante | Este comando permite revertir el control, para conexiones semidúplex |
| 250 | SB | SB | Este comando indica que los datos que siguen son una negociación de la opción anterior. |
| 251 | WILL | Código de opción | |
| 252 | WON'T | Código de opción | |
| 253 | DO | Código de | |

| | | | |
|---|---|---|---|
| | | opción | |
| 254 | DON'T | Código de opción | |
| 255 | IAC | Interpretar como comando | Este comando permite interpretar el byte siguiente como un comando. El comando IAC permite ir más allá de los comandos básicos. |

### Más información

RFC 854 original: http://www.ietf.org/rfc/rfc854.txt

### Analizando TELNET

Lance en su PC-SC el analizador de protocolos Ethereal y póngalo a capturar tramas Ethernet habilitando las opciones de mostrar la captura en tiempo real y scroll automático. Para un mejor análisis de la información capturada, aplique el siguiente filtro:

```
ip.src==10.1.1.XY o ip.dst==10.1.1.XY
```

Abra un terminal e inicie una sesión de Telnet con su máquina virtual asociada.

Pruebe algunos comandos al mismo tiempo que observa la captura, cambie de ruta de directorio, liste archivos, muestre su contenido por pantalla.

Pare la captura de Ethereal y analice cada una de las tramas, identificando los protocolos involucrados.

Identifique algunos de los comandos de control indicados anteriormente.

¿Qué inconveniente encuentra en un acceso remoto a otro equipo mediante este protocolo? ¿Es seguro? ¿Conoce alguna alternativa a Telnet que ofrezca un acceso remoto seguro? Identifíquela con la RFC correspondiente.

Realice una captura de ethereal en la que se aprecie el acceso seguro a su máquina virtual o a cualquier otro equipo del laboratorio.

Checkpoint 7.3: Muestra al profesor de prácticas la diferencia entre un acceso remoto seguro frente al clásico Telnet. ¿Puede utilizar Telnet en los equipos reales del laboratorio?¿Y su equivalente seguro?

Departamento de
Automática y Computación
*Automatika eta*
*Konputazio Saila*

Campus de Arrosadía
*Arrosadiko Campusa*
31006 Pamplona - *Iruñea*
*Tfno. 948 169113, Fax. 948 168924*
*Email: ayc@unavarra.es*

# 4- Protocolos POP3/SMTP

El correo electrónico es considerado el servicio más utilizado de Internet. Por lo tanto, la serie de protocolos TCP/IP ofrece una gama de protocolos que permiten una fácil administración del enrutamiento del correo electrónico a través de la red.

**El protocolo SMTP**

El **protocolo SMTP** (Protocolo simple de transferencia de correo) es el protocolo estándar que permite la transferencia de correo de un servidor a otro mediante una conexión punto a punto.

Éste es un protocolo que funciona en línea, encapsulado en una trama TCP/IP. El correo se envía directamente al servidor de correo del destinatario. El protocolo SMTP funciona con comandos de textos enviados al servidor SMTP (al puerto 25 de manera predeterminada). A cada comando enviado por el cliente (validado por la cadena de caracteres ASCII CR/LF, que equivale a presionar la tecla Enter) le sigue una respuesta del servidor SMTP compuesta por un número y un mensaje descriptivo.

A continuación se describe una situación en la que se realiza una solicitud para enviar correos a un servidor SMTP:

- Al abrir la sesión SMTP, el primer comando que se envía es el comando HELO seguido por un espacio (escrito <SP>) y el nombre de dominio de su equipo (para decir "hola, soy este equipo"), y después validado por Enter (escrito <CRLF>). Desde abril de 2001, las especificaciones para el protocolo SMTP, definidas en RFC 2821, indican que el comando HELO sea remplazado por el comando EHLO.

- El segundo comando es "MAIL FROM:" seguido de la dirección de correo electrónico del remitente. Si se acepta el comando, el servidor responde con un mensaje "250 OK".

- El siguiente comando es "RCPT TO:" seguido de la dirección de correo electrónico del destinatario. Si se acepta el comando, el servidor responde con un mensaje "250 OK".

- El comando DATA es la tercera etapa para enviar un correo electrónico. Anuncia el comienzo del cuerpo del mensaje. Si se acepta el comando, el servidor responde con un mensaje intermediario numerado 354 que indica que puede iniciarse el envío del cuerpo del mensaje y considera el conjunto de líneas siguientes hasta el final del mensaje indicado con una línea que contiene sólo un punto. El cuerpo del correo electrónico eventualmente contenga algunos de los siguientes encabezados:

    - Date (Fecha)
    - Subject (Asunto)
    - Cc
    - Bcc (Cco)
    - From (De)

Campus de Arrosadía
*Arrosadiko Campusa*
31006 Pamplona - *Iruñea*
*Tfno. 948 169113, Fax. 948 168924*
*Email: ayc@unavarra.es*

Si se acepta el comando, el servidor responde con un mensaje "250 OK".

A continuación se describe un ejemplo de transacción entre un cliente(C) y un servidor SMTP(S):

```
S: 220 smtp.commentcamarche.net SMTP Ready C: EHLO machine1.commentcamarche.net
S: 250 smtp.commentcamarche.net C: MAIL FROM:<webmaster@commentcamarche.net> S:
250 OK C: RCPT TO:<meandus@meandus.net> S: 250 C: RCPT TO:<tittom@tittom.fr> S:
550 No such user here C: DATA S: 354 Start mail input; end with <CRLF>.<CRLF> C:
Subject: Hola C: Hola Meandus: C: ¿Cómo andan tus cosas? C: C: ¡Nos vemos pronto!
C: <CRLF>.<CRLF> S: 250 C: QUIT R: 221 smtp.commentcamarche.net closing
transmission
```

Las especificaciones básicas del protocolo SMTP indican que todos los caracteres enviados están codificados mediante el código ASCII de 7 bits y que el 8º bit sea explícitamente cero. Por lo tanto, para enviar caracteres acentuados es necesario recurrir a algoritmos que se encuentren dentro de las especificaciones MIME:

- Base64 para archivos adjuntos
- Quoted-printable (abreviado QP) para caracteres especiales utilizados en el cuerpo del mensaje

Por lo tanto, es posible enviar un correo electrónico utilizando un simple telnet al puerto 25 del servidor SMTP:

```
telnet smtp.commentcamarche.net 25
```

El servidor indicado anteriormente no existe. Intente reemplazar commentcamarche.net por el nombre de dominio de su proveedor de servicios de Internet. Si su proveedor no le permite el acceso por Telnet al puerto 25, diríjase a http://www.terra.es/correo y créese una cuenta con el formato arssXY@terra.es (no le costará más que un par de minutos). Al servidor SMTP accederá mediante `smtp.terra.es`.

A continuación se brinda un resumen de los principales comandos SMTP:

| Comando | Ejemplo | Descripción |
|---|---|---|
| HELO (ahora EHLO) | EHLO 193.56.47.125 | Identificación que utiliza la dirección IP o el nombre de dominio del equipo remitente |
| MAIL FROM: | MAIL FROM: originator@domain.com | Identificación de la dirección del remitente |
| RCPT TO: | RCPT TO: recipient@domain.com | Identificación de la dirección del destinatario |
| DATA | DATA message | Cuerpo del correo electrónico |
| QUIT | QUIT | Salida del servidor SMTP |
| HELP | HELP | Lista de comandos SMTP que el servidor admite |

Todas las especificaciones del protocolo SMTP se encuentran definidas en RFC 821 (desde abril de 2001, las especificaciones del protocolo SMTP se encuentran definidas en RFC 2821).

Departamento de
Automática y Computación
*Automatika eta*
*Konputazio Saila*

Campus de Arrosadía
*Arrosadiko Campusa*
31006 Pamplona - *Iruñea*
*Tfno. 948 169113, Fax. 948 168924*
*Email: ayc@unavarra.es*

## El protocolo POP3

El protocolo POP (Protocolo de oficina de correos), como su nombre lo indica, permite recoger el correo electrónico en un servidor remoto (servidor POP). Es necesario para las personas que no están permanentemente conectadas a Internet, ya que así pueden consultar sus correos electrónicos recibidos sin que ellos estén conectados.

Existen dos versiones principales de este protocolo, POP2 y POP3, a los que se le asignan los puertos 109 y 110 respectivamente, y que funcionan utilizando comandos de texto radicalmente diferentes.

Al igual que con el protocolo SMTP, el protocolo POP (POP2 y POP3) funciona con comandos de texto enviados al servidor POP. Cada uno de estos comandos enviados por el cliente (validados por la cadena CR/LF) está compuesto por una palabra clave, posiblemente acompañada por uno o varios argumentos, y está seguido por una respuesta del servidor POP compuesta por un número y un mensaje descriptivo.

A continuación se brinda un resumen de los principales comandos POP2:

| **Comandos POP2** | |
|---|---|
| Comando | Descripción |
| HELLO | Identificación que utiliza la dirección IP del equipo remitente |
| FOLDER | Nombre de la bandeja de entrada que se va a consultar |
| READ | Número del mensaje que se va a leer |
| RETRIEVE | Número del mensaje que se va a recoger |
| SAVE | Número del mensaje que se va a guardar |
| DELETE | Número del mensaje que se va a eliminar |
| QUIT | Salida del servidor POP2 |

A continuación se brinda un resumen de los principales comandos POP3:

| **Comandos POP3** | |
|---|---|
| Comando | Descripción |
| USER identification | Este comando permite la autenticación. Debe estar seguido del nombre de usuario, es decir, una cadena de caracteres que identifique al usuario en el servidor. El comando USER debe preceder al comando *PASS*. |
| PASS password | El comando *PASS* permite especificar la contraseña del usuario cuyo nombre ha sido especificado por un comando *USER* previo. |
| STAT | Información acerca de los mensajes del servidor |
| RETR | Número del mensaje que se va a recoger |

| | |
|---|---|
| DELE | Número del mensaje que se va a eliminar |
| LIST [msg] | Número del mensaje que se va a mostrar |
| NOOP | Permite mantener la conexión abierta en caso de inactividad |
| TOP <messageID> <n> | Comando que muestra *n* líneas del mensaje, cuyo número se da en el argumento. En el caso de una respuesta positiva del servidor, éste enviará de vuelta los encabezados del mensaje, después una línea en blanco y finalmente las primeras *n* líneas del mensaje. |
| UIDL [msg] | Solicitud al servidor para que envíe una línea que contenga información sobre el mensaje que eventualmente se dará en el argumento. Esta línea contiene una cadena de caracteres denominada *unique identifier listing (lista de identificadores únicos)* que permite identificar de manera única el mensaje en el servidor, independientemente de la sesión. El argumento opcional es un número relacionado con un mensaje existente en el servidor POP, es decir, un mensaje que no se ha borrado. |
| QUIT | El comando *QUIT* solicita la salida del servidor POP3. Lleva a la eliminación de todos los mensajes marcados como eliminados y envía el estado de esta acción. |

Por lo tanto, el protocolo POP3 administra la autenticación utilizando el nombre de usuario y la contraseña. Sin embargo, esto no es seguro, ya que las contraseñas, al igual que los correos electrónicos, circulan por la red como texto sin codificar (de manera no cifrada). En realidad, según RFC 1939, es posible cifrar la contraseña utilizando un algoritmo MD5 y beneficiarse de una autenticación segura. Sin embargo, debido a que este comando es opcional, pocos servidores lo implementan. Además, el protocolo POP3 bloquea las bandejas de entrada durante el acceso, lo que significa que es imposible que dos usuarios accedan de manera simultánea a la misma bandeja de entrada.

De la misma manera que es posible enviar un correo electrónico utilizando telnet, también es posible acceder al correo entrante utilizando un simple telnet por el puerto del servidor POP (110 de manera predeterminada):

```
telnet mail.commentcamarche.net 110
```

El servidor indicado anteriormente no existe. Intente reemplazar `commentcamarche.net` por el nombre de dominio de su proveedor de servicios de Internet. Si su proveedor no le permite el acceso por Telnet al puerto 110, utilice la cuenta arssXY@terra.es creada anteriormente. Si no la creó antes hágalo ahora tal y como se indicó en el apartado anterior.

```
S: +OK mail.commentcamarche.net POP3 service S: (Netscape Messaging Server 4.15
Patch 6 (built Mar 31 2001)) C: USER jeff S: +OK Name is a valid mailbox C: PASS
password S: +OK Maildrop ready C: STAT S: +OK 2 0 C: TOP 1 5 S: Subject: Hola S:
Hola Meandus: S: ¿Cómo andan tus cosas? S: S: ¡Nos vemos pronto! C: QUIT S: +OK
```

La visualización de datos que se obtiene depende del cliente Telnet que esté utilizando. Según su cliente Telnet, puede ser necesario activar la opción echo local (eco local).

Campus de Arrosadía
*Arrosadiko Campusa*
31006 Pamplona - *Iruñea*
*Tfno. 948 169113, Fax. 948 168924*
*Email: ayc@unavarra.es*

### El protocolo IMAP

El protocolo IMAP (Protocolo de acceso a mensajes de Internet) es un protocolo alternativo al de POP3, pero que ofrece más posibilidades:

- IMAP permite administrar diversos accesos de manera simultánea.
- IMAP permite administrar diversas bandejas de entrada.
- IMAP brinda más criterios que pueden utilizarse para ordenar los correos electrónicos.

### Más información

Para obtener más información sobre el protocolo SMTP, consulte RFC821 que explica el protocolo detalladamente: http://www.ietf.org/rfc/rfc821.txt.

Averigüe las RFCs correspondientes a POP3 e IMAP.

### Analizando POP3/SMTP

Realice diversas capturas con ethereal en las que se se muestren los comandos utilizados para el acceso mediante Telnet a los puertos 25 y 110 de su proveedor de correo o de terra.es en caso de haber creado la cuenta correspondiente.

```
telnet pop.proveedor.es 110
```

```
telnet smtp.proveedor.es 25
```

*Nota: Aunque el nombre de dominio asociado a los servidores POP3 y SMTP suelen ser de la forma indicada puede variar de un proveedor a otro, aunque habitualmente siguen esta sintaxis.*

Intente enviar un correo desde su servidor SMTP, ¿Qué errores le muestra?¿A qué se deben? Utilice la interfaz web que le ofrece el proveedor de servicios para el acceso a su correo. Capture mediante ethereal el procedo de envío de un correo y compárelo con el acceso por Telnet.

Deberá ser capaz, en el caso POP3, de listar sus emails, visualizarlos por pantalla y eliminarlos.

A la vista de las capturas realizadas ¿Qué inconveniente presentan POP/SMTP? Averigüe las RFCs correspondientes a los protocolos que proporcionan un envío seguro de correo electrónico.

Checkpoint 7.4: Muestra al profesor de prácticas los resultados obtenidos. Averigüe los puertos que se emplean para el acceso seguro al servicio de correo. Intente realizar una conexión remota a éstos ¿Qué protocolo empleará para ello?

Desde el PC donde se encuentra su máquina virtual, lance WireShark (Ethereal) y utilice el comando `mail` para enviar un correo a la dirección arss0809@gmail.com .Consulte el manual del comando `mail`.

En la captura de WireShark aplique el filtro: `ip.src==10.1.1.XY o ip.dst==10.1.1.XY` ¿Qué observa respecto la captura realizada anteriormente al realizar un Telnet al puerto 25 de su servidor de correo?