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 10 – Protocolos de nivel de aplicación

"Sesión 2"

1- Objetivos

En esta segunda sesión veremos los protocolos HTTP, DNS y SMTP/POP3/IMAP.

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.

4- Protocolo HTTP

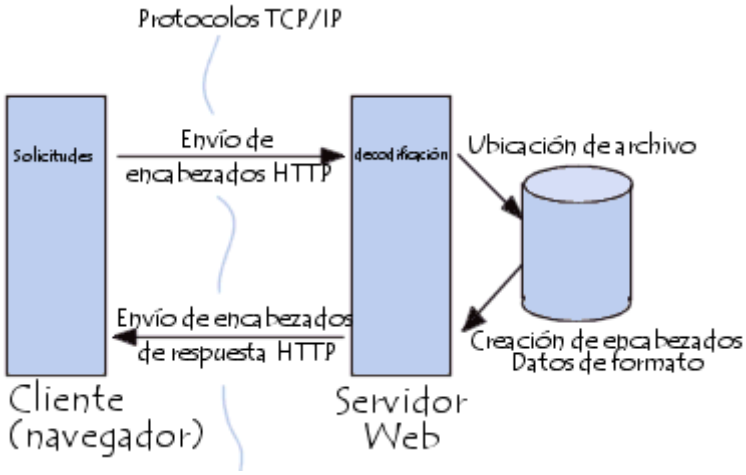
Desde 1990, el protocolo HTTP (Protocolo de transferencia de hipertexto) es el protocolo más utilizado en Internet. La versión 0.9 sólo tenía la finalidad de transferir los datos a través de Internet (en particular páginas Web escritas en HTML). La versión 1.0 del protocolo permite la transferencia de mensajes con encabezados que describen el contenido de los mensajes mediante la codificación MIME. Posteriormente fue mejorada por la versión 1.1

Referencia: http://www2.research.att.com/~bala/papers/h0vh1.html

El propósito del protocolo HTTP es permitir la transferencia de archivos (principalmente, en formato HTML) entre un navegador (el cliente) y un servidor web (por ejemplo, `httpd` en equipos UNIX) localizado mediante una cadena de caracteres denominada dirección URL.

Comunicación entre el navegador y el servidor

La comunicación entre el navegador y el servidor se lleva a cabo en dos etapas:



1. El navegador realiza una solicitud HTTP
2. El servidor procesa la solicitud y después envía una respuesta HTTP

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

En realidad, la comunicación se realiza en más etapas si se considera el procesamiento de la solicitud en el servidor. Sólo nos ocupamos del protocolo HTTP.

Solicitud HTTP

Una solicitud HTTP es un conjunto de líneas que el navegador envía al servidor. Incluye:

Una línea de solicitud: es una línea que especifica el tipo de documento solicitado, el método que se aplicará y la versión del protocolo utilizada. La línea está formada por tres elementos que deben estar separados por un espacio:

- El método
- La dirección URL
- La versión del protocolo utilizada por el cliente (por lo general, HTTP/1.0)

Los campos del encabezado de solicitud: son un conjunto de líneas opcionales que permiten aportar información adicional sobre la solicitud y/o el cliente (navegador, sistema operativo, etc.). Cada una de estas líneas está formada por un nombre que describe el tipo de encabezado, seguido de dos puntos (:) y el valor del encabezado.

El cuerpo de la solicitud: es un conjunto de líneas opcionales que deben estar separadas de las líneas precedentes por una línea en blanco y, por ejemplo, permiten que se envíen datos por un comando POST durante la transmisión de datos al servidor utilizando un formulario.

Una solicitud HTTP posee la siguiente sintaxis (<crlf> retorno de carro y avance de línea):

```
MÉTODO VERSIÓN URL<crlf>
ENCABEZADO: Valor<crlf>
. . . ENCABEZADO: Valor<crlf>
Línea en blanco <crlf>
CUERPO DE LA SOLICITUD
```

A continuación se muestra un ejemplo de una solicitud HTTP:

```
GET http://www.google.es HTTP/1.0 Accept : Text/html If-Modified-Since :
Saturday, 26-May-2009 14:37:11 GMT User-Agent : Mozilla/4.0 (compatible; MSIE
5.0; Windows XP)
```

Comandos

Comando	Descripción
GET	Solicita el recurso ubicado en la URL especificada
HEAD	Solicita el encabezado del recurso ubicado en la URL especificada
POST	Envía datos al programa ubicado en la URL especificada
PUT	Envía datos a la URL especificada
DELETE	Borra el recurso ubicado en la URL especificada

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

Encabezados

Nombre del encabezado	Descripción
Accept	Tipo de contenido aceptado por el navegador (por ejemplo, *texto/html*). Consulte Tipos de MIME
Accept-Charset	Juego de caracteres que el navegador espera
Accept-Encoding	Codificación de datos que el navegador acepta
Accept-Language	Idioma que el navegador espera (de forma predeterminada, inglés)
Authorization	Identificación del navegador en el servidor
Content-Encoding	Tipo de codificación para el cuerpo de la solicitud
Content-Language	Tipo de idioma en el cuerpo de la solicitud
Content-Length	Extensión del cuerpo de la solicitud
Content-Type	Tipo de contenido del cuerpo de la solicitud (por ejemplo, *texto/html*). Consulte Tipos de MIME
Date	Fecha en que comienza la transferencia de datos
Forwarded	Utilizado por equipos intermediarios entre el navegador y el servidor
From	Permite especificar la dirección de correo electrónico del cliente
From	Permite especificar que debe enviarse el documento si ha sido modificado desde una fecha en particular
Link	Vínculo entre dos direcciones URL
Orig-URL	Dirección URL donde se originó la solicitud
Referer	Dirección URL desde la cual se realizó la solicitud
User-Agent	Cadena con información sobre el cliente, por ejemplo, el nombre y la versión del navegador y el sistema operativo

Respuesta HTTP

Una respuesta HTTP es un conjunto de líneas que el servidor envía al navegador. Está constituida por:

Una línea de estado: es una línea que especifica la versión del protocolo utilizada y el estado de la solicitud en proceso mediante un texto explicativo y un código. La línea está compuesta por tres elementos que deben estar separados por un espacio: La línea está formada por tres elementos que deben estar separados por un espacio:

- La versión del protocolo utilizada
- El código de estado

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

- El significado del código

Los campos del encabezado de respuesta: es un conjunto de líneas opcionales que permiten aportar información adicional sobre la respuesta y/o el servidor. Cada una de estas líneas está compuesta por un nombre que califica el tipo de encabezado, seguido por dos puntos (:) y por el valor del encabezado Cada una de estas líneas está formada por un nombre que describe el tipo de encabezado, seguido de dos puntos (:) y el valor del encabezado.

El cuerpo de la respuesta: contiene el documento solicitado.

Por lo tanto, una respuesta HTTP posee la siguiente sintaxis (<crlf> significa retorno de carro y avance de línea):

```
VERSIÓN-HTTP CÓDIGO EXPLICACIÓN <crlf>
ENCABEZADO: Valor<crlf>
. . . ENCABEZADO: Valor<crlf>
Línea en blanco <crlf>
CUERPO DE LA RESPUESTA
```

A continuación se muestra un ejemplo de una respuesta HTTP:

```
HTTP/1.0 200 OK Date: Tue, 26 May 2009 14:37:12 GMT Server : Microsoft-IIS/2.0
Content-Type : text/HTML Content-Length : 1245 Last-Modified : Tue, 26 May
2009 08:25:13 GMT
```

Encabezados de respuesta

Nombre del encabezado	Descripción
Content-Encoding	Tipo de codificación para el cuerpo de la respuesta
Content-Language	Tipo de idioma en el cuerpo de la respuesta
Content-Length	Extensión del cuerpo de la respuesta
Content-Type	Tipo de contenido del cuerpo de la respuesta (por ejemplo, *texto/html*). Consulte Tipos de MIME
Date	Fecha en que comienza la transferencia de datos
Expires	Fecha límite de uso de los datos
Forwarded	Utilizado por equipos intermediarios entre el navegador y el servidor
Location	Redireccionamiento a una nueva dirección URL asociada con el documento
Server	Características del servidor que envió la respuesta

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

Los códigos de respuesta

Son los códigos que se ven cuando el navegador no puede mostrar la página solicitada. El código de respuesta está formado por tres dígitos: el primero indica el estado y los dos siguientes explican la naturaleza exacta del error.

Código	Mensaje	Descripción
10x	**Mensaje de información**	**Estos códigos no se utilizan en la versión 1.0 del protocolo**
20x	**Éxito**	**Estos códigos indican la correcta ejecución de la transacción**
200	OK	La solicitud se llevó a cabo de manera correcta
201	CREATED	Sigue a un comando POST e indica el éxito, la parte restante del cuerpo indica la dirección URL donde se ubicará el documento creado recientemente.
202	ACCEPTED	La solicitud ha sido aceptada, pero el procedimiento que sigue no se ha llevado a cabo
203	PARTIAL INFORMATION	Cuando se recibe este código en respuesta a un comando de GET indica que la respuesta no está completa.
204	NO RESPONSE	El servidor ha recibido la solicitud, pero no hay información de respuesta
205	RESET CONTENT	El servidor le indica al navegador que borre el contenido en los campos de un formulario
206	PARTIAL CONTENT	Es una respuesta a una solicitud que consiste en el encabezado *range*. El servidor debe indicar el encabezado *content-Range*
30x	**Redirección**	**Estos códigos indican que el recurso ya no se encuentra en la ubicación especificada**
301	MOVED	Los datos solicitados han sido transferidos a una nueva dirección
302	FOUND	Los datos solicitados se encuentran en una nueva dirección URL, pero, no obstante, pueden haber sido trasladados
303	METHOD	Significa que el cliente debe intentarlo con una nueva dirección; es preferible que intente con otro método en vez de GET
304	NOT MODIFIED	Si el cliente llevó a cabo un comando GET condicional (con la solicitud relativa a si el documento ha sido modificado desde la última vez) y el documento no ha sido modificado, este código se envía como respuesta.
40x	**Error debido al cliente**	**Estos códigos indican que la solicitud es incorrecta**
400	BAD REQUEST	La sintaxis de la solicitud se encuentra formulada de manera errónea o es imposible de responder
401	UNAUTHORIZED	Los parámetros del mensaje aportan las especificaciones de formularios de autorización que se admiten. El cliente debe reformular la solicitud con los datos de autorización correctos
402	PAYMENT REQUIRED	El cliente debe reformular la solicitud con los datos de pago correctos

403	FORBIDDEN	El acceso al recurso simplemente se deniega
404	NOT FOUND	Un clásico. El servidor no halló nada en la dirección especificada. Se ha abandonado sin dejar una dirección para redireccionar... :)
50x	**Error debido al servidor**	**Estos códigos indican que existe un error interno en el servidor**
500	INTERNAL ERROR	El servidor encontró una condición inesperada que le impide seguir con la solicitud (una de esas cosas que les suceden a los servidores...)
501	NOT IMPLEMENTED	El servidor no admite el servicio solicitado (no puede saberlo todo...)
502	BAD GATEWAY	El servidor que actúa como una puerta de enlace o proxy ha recibido una respuesta no válida del servidor al que intenta acceder
503	SERVICE UNAVAILABLE	El servidor no puede responder en ese momento debido a que se encuentra congestionado (todas las líneas de comunicación se encuentran congestionadas, inténtelo de nuevo más adelante)
504	GATEWAY TIMEOUT	La respuesta del servidor ha llevado demasiado tiempo en relación al tiempo de espera que la puerta de enlace podía admitir (excedió el tiempo asignado...)

Analizando HTTP

Nota: *no haga nada hasta terminar de leer el apartado completo (hasta el checkpoint 10.3)*

Lance en su PC-SC el analizador de protocolos Wireshark y póngalo a capturar tramas Ethernet. Para un mejor análisis de la información capturada, aplique el siguiente filtro:

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

Abra su navegador y escriba como URL: http://10.1.1.XY

Verá la página de inicio del servidor Apache que está corriendo en su máquina virtual.

Pare la captura de Wireshark y analice cada una de las tramas, identificando los protocolos presentes. Guarde su captura, la necesitará enseguida.

Vuelva a activar Wireshark.

Conéctese mediante `telnet` a su máquina virtual en el puerto correspondiente al servicio http. Para ver los puertos asociados a los distintos servicios, consulte el fichero `/etc/services` en el propio PC-SC.

Una vez conectado, teclee el comando: GET / http/1.1 y pulse ENTER dos veces. Si no obtiene la página del servidor Apache, indique tras la petición GET, en una segunda línea, el nombre de host correspondiente y vuelva a pulsar ENTER dos veces.

Guarde su captura y compárela con la obtenida al utilizar el navegador, ¿Qué diferencias encuentra? ¿A qué se deben?

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

Utilicen la información proporcionada por la página web genérica del servidor Apache de su máquina virtual para ubicar en ésta, una página html sencilla que pueda descargar desde el PC-SC. Si no está familiarizado con el html, siga los siguientes pasos:

```
#vi pagina<n°armario>.html
```

Pulse la tecla "Insert" para activar el modo edición del editor `vi`. Teclee el siguiente texto:

```
<html>
   <head>
         <title>Arquitectura de Redes Sistemas y Servicios</title>
   </head>
   <body>
         Laboratorio de Telemática I – Práctica 10
   </body>
</html>
```

Pulse la tecla "Esc", teclee `:wq (write & quit)` y pulse "ENTER".

Ya tiene un página html, ahora sólo tiene que llevarla a su máquina virtual y ubicarla en la carpeta que se indica en la página web por defecto del servidor Apache. Utilice el servicio que crea conveniente para ello (recuerde que también podría editar su página html directamente en la máquina virtual).

Nota: habitualmente la carpeta `/var/www/html/` tiene permisos de `root`. Éstos se han modificado para que cualquier usuario del sistema pueda publicar su propia página web.

Checkpoint 10.3: Muestra al profesor de prácticas que, mediante una conexión Telnet a su máquina virtual desde el PC-SC, es capaz de cargar la página creada. Descargue también su encabezado.

Vuelva a lanzar wireshark con el mismo filtro anterior y descargue mediante su navegador la página `http://10.1.1.XY/arsswww/pagina-arss.html`

Analice las tramas capturadas y justifique si se ha usado HTTP persistente y por qué.

Analizando DNS

Ponga Wireshark a capturar con el filtro adecuado. En esta ocasión le interesará filtrar por ip origen o destino la de su PC-SC y además por el protocolo DNS.

Lance un ping de un solo paquete a www.terra.es

Pare la captura y analice las tramas correspondientes al servicio dns. ¿Cuántas peticiones y respuestas ha obtenido? ¿Cuál es la dirección IP del dns del laboratorio? ¿Cuál es el puerto asociado al servicio de nombres? ¿Qué servidores de nombre aparecen en la trama de respuesta?

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 SMTP/POP3/IMAP

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.

Se describe a continuación una solicitud para enviar correo mediante 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)

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? ¡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, ***utilice como contraseña "arssXY"***). Servidores de correo de terra.es: http://www.terra.es/usuarios/config/outlook-email.htm

A continuación se muestra 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).

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 muestra 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 muestra 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

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? ¡Nos vemos pronto!
C: QUIT
S: +OK
```

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

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 y recuerde ***utilice como contraseña "arssXY".*** Servidores de correo de terra.es: http://www.terra.es/usuarios/config/outlook-email.htm

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).

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 ofrece 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 Wireshark 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 Wireshark el proceso 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 10.4: 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?