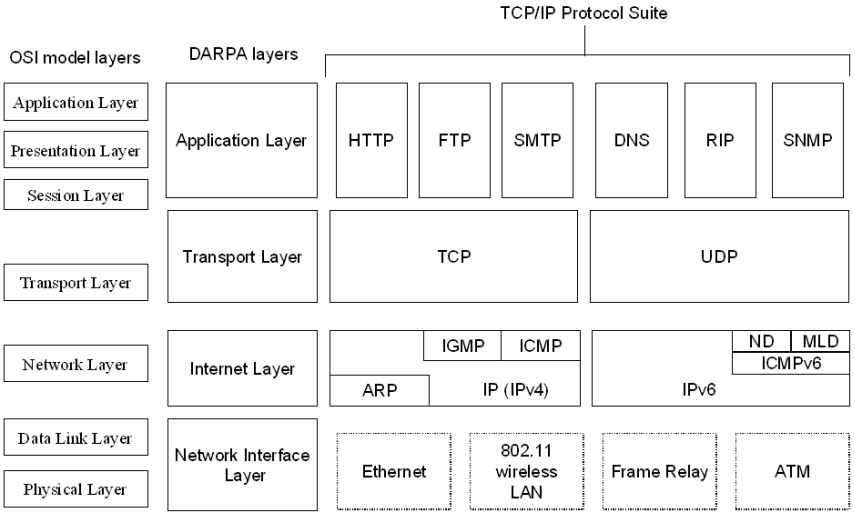
Nombre: .....

Fecha: /02/2012 Grupo: 1 □

PRÁCTICA 5
INTERNET. PROTOCOLOS DE LA PILA TCP/IP.

En esta práctica vamos a tratar de explicar cómo funciona la pila de protocolos TCP/IP, que nos permiten las comunicaciones a través de Internet. La pila TCP/IP recibe su nombre de los protocolos TCP (Transmission Control Protocol) e IP (Internet Protocol), pero involucra a muchos más protocolos, que generalmente se representan, y se pueden entender, como una pila formada por diversas capas.



En lo que a nosotros respecta, sólo prestaremos atención a la segunda ("DARPA layers") y tercera ("TCP/IP Protocol Suite") columnas de la anterior imagen. La segunda columna representa los cuatro niveles de la pila TCP/IP (capa de aplicación, capa de transporte, capa de Internet y capa física o de red). La tercera, enumera (algunos de) los protocolos que podemos encontrar en cada una de las capas (por ejemplo, http y ftp en la capa de aplicación, donde también se encuentran pop o imap, tcp y udp en la capa de transporte, IPv4, IPv6 o ARP en la capa de Internet y Ethernet y algunos otros en la capa física).

En las siguientes prácticas trataremos de ilustrar cómo funcionan algunos de los protocolos, la diferencia entre el papel de las distintas capas y cómo se produce la comunicación de datos entre máquinas en Internet. En particular, en la práctica de hoy, prestaremos atención a la capa de aplicación y algunos de sus protocolos.

1. En primer lugar, vamos a ver cómo podemos acceder a recursos que están disponibles a través de Internet, conociendo tanto el protocolo por el que están accesibles como su ruta.

Abre 7 pestañas del navegador Mozilla Firefox y copia en cada una de ellas las siguientes rutas:

C:
www.uca.edu.sv/investigacion/tutoriales/tcp-ip.html
http://www.uca.edu.sv/investigacion/tutoriales/tcp-ip.html
www.uca.edu.sv/investigacion/tutoriales/tcp-ip2.gif
ftp.epson.com/laser/ACTLQA.TXT
ftp://ftp.epson.com/laser/ACTLQA.TXT
ftp://ftp.epson.com/laser/LASERIJ.GIF

Responde a las siguientes preguntas en tu informe. ¿A qué tipo de recursos (tipos de archivo) has podido acceder por medio de tu navegador? ¿Qué protocolos de aplicación es capaz de reconocer? ¿Qué protocolos ha sido capaz de inferir incluso sin nuestra ayuda (sin consignar nosotros el nombre del protocolo)?

Abrimos ahora Paint (lo puedes encontrar escribiendo Paint en la barra del menú para buscar programas y archivos). Trata de acceder (Archivo -> Abrir) a las siguientes direcciones:

http://www.uca.edu.sv/investigacion/tutoriales/tcp-ip.html
http://www.uca.edu.sv/investigacion/tutoriales/tcp-ip2.gif
ftp://ftp.epson.com/laser/ACTLQA.TXT
ftp://ftp.epson.com/laser/LASERIJ.GIF

¿Qué formatos de archivo reconoce Paint? ¿Es capaz Paint de trabajar con recursos a través de su dirección web?

Vamos a repetir la misma prueba con el bloc de notas. Trata de acceder a las siguientes direcciones:

http://www.uca.edu.sv/investigacion/tutoriales/tcp-ip.html
http://www.uca.edu.sv/investigacion/tutoriales/tcp-ip2.gif

¿Qué formatos de archivo reconoce notepad? ¿Es capaz notepad de trabajar con recursos a través de su dirección web?

Finalmente ejecuta Filezilla, y trata de acceder a las siguientes direcciones (copia también la parte correspondiente al protocolo "http://" o "ftp://"):

http://www.uca.edu.sv/investigacion/tutoriales/tcp-ip.html
ftp://ftp.epson.com/laser/ACTLQA.TXT

Comenta lo que ha sucedido en cada uno de los dos casos.

2. Vamos a tratar de entender ahora un poco mejor cómo son las direcciones que nos permiten acceder a recursos a través de Internet. Estas direcciones se conocen como URL's (Uniform Resource Locator) o URI's (Uniform Resource Identifier), y ya las hemos utilizado, por ejemplo, para definir los enlaces a páginas web en HTML.

Observa por ejemplo el siguiente enlace:

http://es.wikipedia.org/w/wiki.phtml?title=URL&action=history

Accede a la página señalada. Generalmente las url's responden al siguiente esquema:

protocolo://máquina.dominio:puerto/camino/fichero?parámetros

El protocolo puede ser alguno entre http (protocolo de transferencia de hipertexto), https (protocolo seguro de transferencia de hipertexto), ftp (protocolo de transferencia de ficheros), smtp (protocolo simple de transferencia de correo), pop (protocolo de la oficina de correo), ldap (protocolo ligero de acceso a directorios), file (para archivos disponibles en la máquina local), telnet… La máquina y el dominio conforman la parte más identificable de una url. Por ejemplo, en https://belenus.unirioja.es, belenus es un servidor (o un subdominio) dentro del dominio "unirioja.es". Los puertos están relacionados con el protocolo TCP. El camino especifica la ruta del recurso solicitado en su servidor. El fichero es el recurso solicitado, y la lista de parámetros nos permiten enviarle información modificando así su respuesta.

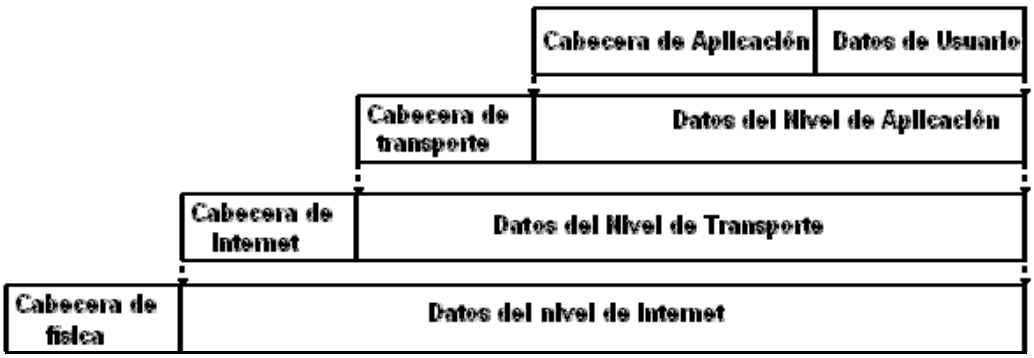
En tu informe de la práctica identifica cada una de esas partes en la url http://es.wikipedia.org/w/wiki.phtml?title=URL&action=history.

Toma la dirección anterior de la wikipedia http://es.wikipedia.org/w/wiki.phtml?title=URL&action=history y en la barra del navegador realiza las siguientes modificaciones. Explica en el informe el resultado (después de cada modificación recupera la url original):

- Modifica el protocolo "http" por "https" y recarga la página.
- Cambia "es" por "ES" y recarga la página.
- Cambia "wikipedia" por "WIKIPEDIA" y recarga la página.
- Cambia "es.wikipedia.org" por "es.wikipedia.org:80" y recarga la página.
- Cambia "es.wikipedia.org" por "es.wikipedia.org:81" y recarga la página (¿cuál es el puerto por defecto del protocolo http?).
- Cambia "/w/" por "/W/" y recarga la página.
- Cambia "URL" por "Logroño" y recarga la página.
- Cambia "history" por "History" y recarga la página.

3. La información a través de Internet se comunica por medio de paquetes. Igual que decíamos que en un disco duro la unidad mínima de memoria era un sector, y en un sistema de archivos la unidad mínima de memoria era un clúster, en Internet dicha unidad recibe el nombre de paquete. Cada vez que hacemos una solicitud de un recurso en Internet, estamos generando uno o varios paquetes que contienen la misma (y que serán encaminados a su destino por un "router"). La respuesta que recibamos también estará formada por paquetes que nuestro programa cliente (dependiente del protocolo que usemos, ftp, http, pop, smtp…) convertirá en una página web, un mensaje de correo, una imagen o un fichero.

Los paquetes se construyen de la siguiente forma. A una petición que hagamos en el navegador, o a su respuesta desde el servidor, se le asignará en primer lugar una "cabecera de aplicación". La misma contendrá información referente al protocolo usado (de los de la capa de aplicación), al método en que se ha solicitado el recurso (GET, POST…), al agente de usuario (Mozilla…), a la máquina huésped del recurso…



Las restantes capas añaden información referente a puertos, IPs, direcciones ETHERNET….

Por el momento, vamos a tratar de analizar los paquetes que se generan en nuestra máquina para los protocolos de la capa de aplicación. Para ello haremos uso de "Wireshark" (http://www.wireshark.org/). Puedes comprobar si el programa está instalado en tu ordenador, y si no descargarlo (versión de 32 bits) e instalarlo. Ejecútalo. Sería conveniente que cerraras todas las pestañas del navegador para no generar más tráfico adicional.

Para poder hacer uso de "Wireshark", debemos elegir cuál de las interfaces de red de nuestro ordenador (inalámbrica, de cable, interna…) queremos "capturar". Dentro del menú "Capture", opción "Interfaces", comprueba cuál de las interfaces presenta una mayor actividad (debería de ser la "Network Connection") y pulsa la tecla "Start".

Verás que en tu pantalla empiezan a aparecer todos los paquetes que están pasando por tu ordenador (aunque pueda parecer que no haya ninguna actividad de red).

Como puedes observar, la cantidad de información que puede llegar a generar el programa es ingente, así que tendremos que ser selectivos con la misma. Para ello haremos uso de la ventana "Filter".

En primer lugar, abre una consola de MSDOS ("cmd") y ejecuta el comando "ipconfig" y averigua la dirección IP de tu ordenador (la correspondiente a "Adaptador de Ethernet - Conexión de área local"). Anótala en tu informe de prácticas.

Ahora abre en una ventana de tu navegador la página web http://www.rfc-es.org/rfc/rfc1034-es.txt.

Antes de abrir cualquier sitio web, nuestro ordenador hace una solicitud a un servidor DNS (domain name server) para que el mismo le diga cuál es la dirección IP de la máquina en la que está alojado dicho sitio web. Aunque nosotros no seamos conscientes de ello, hay un protocolo DNS (que pertenece a la capa de aplicación) que se encarga de dicha petición. En la ventana "Filter" de Wireshark, escribe "dns" y pulsa "Apply". Observa los resultados.

Trata de encontrar el mensaje "Standard-query A www.rfc-es.org" y la respuesta al mismo, "Standard-query response A …".

Escribe en tu informe cuáles son las IPs "Source" y "Destination" de ambos mensajes.

Selecciona el primer mensaje de ambos, y pulsa sobre el mismo el botón derecho de tu ratón. Elige la opción "Show Packet in New Window". La parte superior de la ventana mostrará la estructura del paquete. Leeremos la misma de abajo hacia arriba:

- El mensaje en "Domain Name System (query)" se corresponde con el mensaje generado en la capa de aplicación. Trata de desplegarlo pulsando sobre el símbolo "+" que aparece a la izquierda del mismo. Del mensaje que aparece, la parte que más nos interesa es la correspondiente a "Queries". Ahí podemos ver el nombre de dominio que debe ser resuelto por el servidor DNS. Anota el nombre de la "query" en tu informe de la práctica. El resto de información son cabeceras que añade el protocolo DNS (datos adicionales para el servidor de destino).

- El mensaje en "User Datagram Protocol" corresponde con el mensaje generado al pasar el mensaje de "Domain Name System (query)" por la capa de transporte. Si te fijas, observarás que ha aparecido información sobre los puertos de origen "Src" y destino "Dst". Anótalos en el informe.

- El mensaje en "Internet Protocol" corresponde con el mensaje generado al pasar el mensaje de "User Datagram Protocol" por la capa de Internet. Al mensaje se le ha añadido ya una IP de origen (la de tu máquina) y una IP de destino (la del servidor DNS). Anota ambas direcciones IP en tu informe.

- Finalmente, el mensaje en "Ethernet II" corresponde con el mensaje generado al pasar el mensaje propio de la parte "Internet Protocol" por la capa física. En el mismo se han añadido las direcciones MAC (Media Access Control address) de tu máquina y del servidor DNS al mensaje. Anota ambas direcciones en el informe de la práctica.

Al mensaje generado, el servidor DNS ha respondido con el mensaje "Standard query response A…". Abre dicho mensaje, y en la parte "Domain Name System (response)" identifica la pregunta ("query") que le has realizado al servidor, y la respuesta ("response") que te ha enviado el mismo. Anota la dirección IP de www.rfc-es.org.

4. Vamos a centrarnos ahora en la comunicación que ha habido entre nuestro ordenador y la página web que hemos abierto (http://www.rfc-es.org/rfc/rfc1034-es.txt).

Dentro de la ventana "Filter" de Wireshark escribe el siguiente filtro:

ip.addr eq la_ip_de_tu_equipo and ip.addr eq la_ip_de_www.rfc-es.org

El anterior comando nos permite filtrar todos los paquetes que se han comunicado entre tu máquina y el servidor de "www.rfc-es.org".

De los mensajes filtrados, deberías identificar un mensaje de protocolo "HTTP" cuya "Info" corresponda con "GET /rfc/rfc1034-es.txt". Ese mensaje es la solicitud de recursos que tu ordenador le ha hecho al servidor (recuerda que primero DNS ha tenido que resolver la dirección del servidor). Pulsa sobre ese mensaje con el botón derecho y elige la opción "Follow TCP Stream" (también puedes hacer "Show Packet in New Window" si quieres estudiar el paquete enviado). La opción "Follow TCP Stream" nos muestra la comunicación, en ambas direcciones, que ha habido entre nuestra máquina y el servidor. En la ventana generada por "Follow TCP Stream" puedes observar en rojo las cabeceras HTTP (cabeceras de la capa de aplicación) que tu ordenador ha generado, y en azul las respuestas del servidor.

Anota en el informe los campos (no sus valores) que hay en la cabecera de aplicación que tu ordenador ha generado.

Vuelve ahora al resultado del filtro y consigue encontrar un mensaje cuyo "Protocol" sea "HTTP" y cuya "Info" sea "http/1.1 200 OK (text/plain)". Con el botón derecho elige "Show Packet in New Window". ¿Cuál es el contenido de su parte "Lined-based text data"?

En realidad, el mensaje anterior era demasiado largo para el tamaño de un paquete, y el mismo se ha compuesto de varios paquetes "TCP" que el ordenador después ha recompuesto (lo puedes comprobar en "Reassembled TCP Segments").

5. Acabamos de comprobar cómo se puede entender una sesión "http" desde el punto de vista de los protocolos de aplicación. Vamos a hacer ahora lo mismo con una sesión "ftp".

Asegúrate de que Wireshark sigue capturando los paquetes (lo puedes comprobar en la barra inferior de la aplicación, si el campo "Packets" cambia cada poco tiempo de valor).

Ejecuta "filezilla". Abre una sesión en belenus con el usuario y contraseña de tu CUASI. Abre el directorio "public_html" y descarga el fichero "index.htm" a tu ordenador.

Ahora dirígete a Wireshark. En la ventana "filter" escribe "ftp" y pulsa "Apply". Selecciona el primer mensaje de la comunicación. Escribe en tu informe las IPs de origen y destino del mismo. Abre el mensaje. Anota los

niveles o capas que identificas en el mensaje (sólo su nombre, no los detalles). ¿Cuáles coinciden con las del mensaje que hemos analizado en http? ¿Cuáles son los puertos e IP's de origen y destino de la comunicación ftp? ¿Cuáles son las MAC correspondientes?

Vuelve a la pantalla del filtro. Trata de seguir la sesión ftp que has realizado por la lista de paquetes que tienes en pantalla. ¿Puedes observar tu usuario y contraseña en la misma? ¿Están encriptados?

6. Ahora filtra los paquetes de Wireshark por el protocolo "ftp-data". ¿Qué paquetes observas? ¿Cuál es su contenido?

7. Tanto ftp como http o dns son protocolos de los más comunes de la capa de aplicación. Comprueba en la siguiente url algunos otros protocolos de la capa de aplicación y apunta su nombre en tu guión de la práctica: http://es.wikipedia.org/wiki/Capa_de_aplicaci%C3%B3n.

Vamos a ver algunas herramientas que nos permiten conocer si los distintos dispositivos de una red están funcionando adecuadamente.

8. Vamos a utilizar una aplicación llamada "ping". El programa "ping" es una utilidad que se usa para diagnosticar el estado de una red (por ejemplo, que nuestro ordenador es capaz de conectarse a Internet, o que la página a la que nos queremos conectar es accesible). Para ello, el programa envía paquetes de datos a la máquina de destino, y espera que la misma devuelva los mismos datos.

Vamos a comprobar cómo funciona. Ejecuta "cmd" (la consola de MSDOS):

- Ejecuta el mandato "ping 88.221.92.8".
- Ejecuta el mandato "ping 10.0.1.31". Anota el resultado (positivo o negativo).
- Ejecuta el mandato "ping www.uned.es". Anota el resultado y la IP de la máquina de destino.

Que un servidor no responda a una petición por "ping" puede deberse a varios motivos. Uno es que el servidor no esté disponible. Otro, muy común, es que el servidor prohíba las solicitudes por "ping" porque las mismas podrían dar lugar a un ataque de denegación de servicio sobre el servidor (http://es.wikipedia.org/wiki/Ataques_de_denegaci%C3%B3n_de_servicio, http://es.wikipedia.org/wiki/Ping_de_la_muerte, http://es.wikipedia.org/wiki/Ping_flood).

9. Vamos a hacer uso ahora de una segunda aplicación, "tracert", que nos permite seguir la ruta que sigue un paquete que sale de nuestra máquina dirigido a otra. También provee información sobre la "distancia" (en tiempo) entre nuestra máquina y el servidor requerido.

En la consola de MSDOS:

- Ejecuta "tracert 88.221.92.8". ¿Por cuántos servidores ha pasado el mensaje antes de llegar a destino? ¿Cuál es la primera dirección a la que

llega el mensaje cuando sale de tu máquina? ¿Cuántos de esos pasos han sido en la red local (IP 10. … . … . …)?
- Ejecuta "tracert 10.0.1.31" (ahora el servidor DNS no actúa).
- Ejecuta "tracert www.uned.es". ¿Por cuántos servidores ha pasado el mensaje antes de llegar a destino? ¿Cuál es la primera dirección a la que llega el mensaje cuando sale de tu máquina? ¿Cuántos de esos pasos han sido en la red local (IP 10. … . … . …)?

En el último de los casos, apunta la última dirección IP a la que ha llegado nuestro mensaje. Esa dirección será la puerta de entrada a la red en la que se encuentra la máquina donde se aloja el servidor www.uned.es.

A continuación vamos a visitar la página web de la entidad que se encarga de gestionar los nombres de dominios para nuestro país, en este caso en particular los nombres cuya extensión es ".es", y observar los pasos necesarios para reservar un dominio.

10. Visita la página web www.nic.es. NIC (Network Information Center) es la entidad encargada de asignar los nombres de dominios de Internet a personas o empresas para que los mismos, a través de un DNS, puedan montar sus sitios web mediante un proveedor de hospedaje.

Consulta en www.nic.es algunos dominios y observa cuál es el proceso y la información necesaria para el registro de los mismos. Comprueba también algunos dominios conocidos (unirioja.es, reinaleonor.es, a-prima.es) y los datos de sus propietarios, que son públicos.

De nuevo vamos a volver a explorar la utilidad de los servidores DNS, en particular, cómo podemos cambiarlos y qué sucede cuando utilizamos direcciones incorrectas.

11. Vamos ahora a la configuración de red de tu ordenador ("Panel de Control->Redes e Internet->Ver el estado y las tareas de red->Conexión de área local->Propiedades->Protocolo de Internet Versión 4->Propiedades"). Modifica las direcciones de los servidores DNS. Escribe, por ejemplo, "1.1.1.1" y "2.2.2.2.". Cierra y guarda la configuración. En tu navegador trata de abrir una página web cualquiera. Anota en tu informe el nombre de la página y el error que has encontrado.

Restituye la configuración de los servidores DNS a su estado original.

En la siguiente página puedes conseguir direcciones de servidores DNS. Entra en http://www.adslayuda.com/index.php?module=FSDns&order=info y anota la dirección de algunos de los servidores DNS de los que hay disponibles. Anótalas en tu informe de prácticas.

Si los servidores DNS no están bien configurados, el ordenador no es capaz de resolver ningún nombre de dominio, evitando que podamos navegar por la red (a no ser que conozcamos las IPs de las máquinas que queremos visitar; prueba a abrir en tu navegador la IP de la página www.rae.es con los servidores DNS mal configurados y observa el resultado).