Nombre: ..... Fecha: / 10 /2010

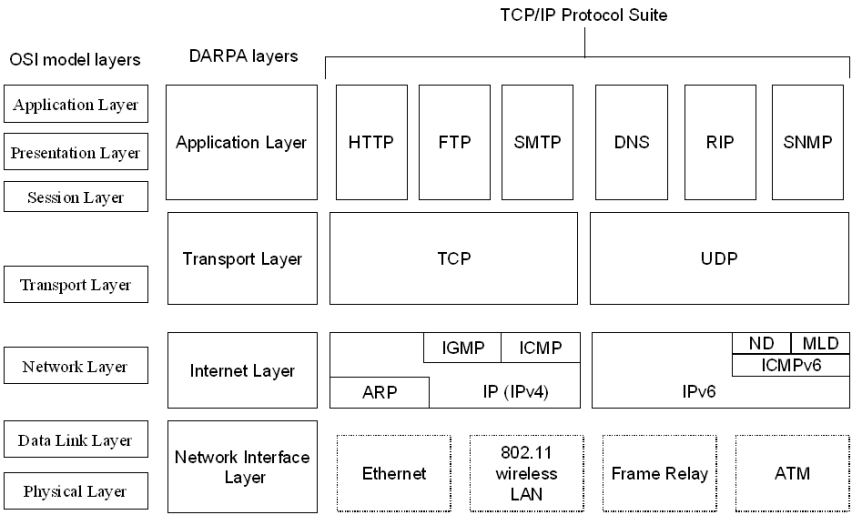
Grupo: 1 ☐ 2 ☐ 3 ☐ 4 ☐

PRÁCTICA 10
INTERNET. CAPA FÍSICA. PROTOCOLOS DE CORREO.

En la tercera práctica sobre protocolos de correo TCP/IP vamos a prestar atención a la capa física de los protocolos de Internet y a algunos de los protocolos más comunes para el envío y recepción de correo electrónico.

Dentro de la capa física nos detendremos sólo en el protocolo Ethernet, que es el más extendido para interconectar redes LAN (Local Area Network). Veremos ciertos detalles que nos permitirán ver las cabeceras de los mensajes, y cómo se produce el tráfico en (y entre) redes.

Con respecto al correo electrónico, existen tres protocolos que son los más extendidos (POP, SMTP e IMAP) y aprenderemos su funcionamiento y configuración con el uso de un cliente de correo electrónico.



1. Ethernet es un protocolo de la capa física de la pila TCP/IP. Su funcionamiento está basado en el uso de tarjetas de red que contienen una dirección MAC (Media Access Control) de 6 bytes que es única para cada dispositivo.

Instalamos Wireshark en nuestro ordenador y comenzamos una nueva captura de la interfaz de red "Network Protocol". Puedes filtrar el tráfico por tu ip ("ipconfig" en "cmd"). Abre la página www.w3c.org. Filtra el tráfico DNS de tu máquina ("Filter: dns") y averigua la IP de www.w3c.org. Ahora filtra el tráfico entre tu ip y la de www.w3c.org ("Filter: ip.addr eq ip_de_tu_maquina and ip.addr eq ip_de_www.w3c.org"). Selecciona uno de los paquetes http de la comunicación que se hayan originado en tu ordenador (por ejemplo el que contiene el GET de la página HTML) y tengan como destino la máquina que aloja www.w3c.org. Abre el paquete y apunta en tu informe de la práctica las direcciones MAC (dentro de la cabecera correspondiente a Ethernet) tanto de tu máquina como del servidor de destino. Apunta en tu informe qué información adicional (o cabeceras) aparece en las cabeceras el protocolo Ethernet, así como si el mismo es un

protocolo orientado a conexión (¿existe algún campo en la cabecera de Ethernet que te permite guardar traza de cómo tiene lugar el tráfico?).

Abrimos ahora la página www.rae.es y capturamos el paquete http que contiene la petición GET hecha al servidor (puedes seguir el mismo proceso que con www.w3c.org). De nuevo apuntamos sus cabeceras Ethernet (en particular, la dirección de la tarjeta MAC del servidor de destino del paquete).

Compáralo con la información de las cabeceras Ethernet del paquete filtrado en la comunicación con www.w3c.org. ¿Qué observas? ¿Tienes alguna explicación para lo mismo?

En general, las redes LAN (Local Area Network) están configuradas de tal forma que todas las máquinas dentro de la misma acceden al exterior a través de una misma máquina (una especie de router que se suele llamar puerta de enlace o "gateway" http://es.wikipedia.org/wiki/Gateway_(inform%C3%A1tica)). Esta máquina es a la que va dirigido todo nuestro tráfico (a nivel del protocolo Ethernet). Ella se encarga también de capturar todo el tráfico del exterior que va dirigido a nuestra LAN y repartirlo adecuadamente. Simplemente como curiosidad, esta máquina debe tener 2 tarjetas de red, una hacia la red interna (en este caso la sala de prácticas) y otra hacia el exterior.

Para poder saber cuál es la dirección (IP) de la puerta de enlace de tu red, puedes hacer uso del protocolo ARP (Address Resolution Protocol). ¿A qué capa de la pila TCP/IP pertenece el mismo? Puedes leer algo más sobre el mismo en http://es.wikipedia.org/wiki/Address_Resolution_Protocol.

Otra forma de averiguar la dirección de la puerta de enlace es por medio del comando "ipconfig/all". Ejecuta el anterior comando en la consola "cmd" y apunta la dirección de la puerta de enlace predeterminada en el informe de la práctica. Compárala con la de tus compañeros.

2. Vamos ahora a intentar averiguar cuál es la dirección IP de nuestra máquina. Hemos visto hasta ahora una forma rápida de conseguirlo, consistente en ejecutar "cmd" y posteriormente "ipconfig". Esto nos dará información sobre nuestra IP dentro de la red LAN en que nos encontremos, pero no será la IP que utilicemos fuera de la LAN (recuerda lo que pasaba con la IP de www.unirioja.es cuando le hacíamos un "ping" desde dentro de la red de la Universidad y cuando hacíamos un "nslookup" con un servidor DNS externo).

Abre en el navegador la dirección www.knowmyip.com y apunta el número de IP y el nombre de dominio (o "hostname"). Compáralo con el de tus compañeros. Trata de dar una explicación a ese hecho en tu informe de prácticas.

Responde en tu informe de prácticas a las siguientes preguntas ¿A qué dirección IP iban dirigidos todos los paquetes que vimos en la práctica 9 sobre la capa de Internet del protocolo TCP/IP? ¿A la IP local de tu máquina o a la IP "pública" de tu máquina? ¿Quién se ha encargado de "solucionar" el desfase entre las cabeceras IP que salen de tu máquina y los mensajes

que recibes? El encargado de todas esas operaciones ha sido el router que hace el papel de Gateway. Puedes encontrar algunos detalles sobre el mismo, y sobre el mecanismo NAT (Network Address Translation) en http://es.wikipedia.org/wiki/Network_Address_Translation.

Pasamos ahora a trabajar con protocolos de correo.

3. Accede a la dirección http://www.unirioja.es/servicios/si/red_servidores/correo/. Lee la información de manejo y configuración de la cuenta de correo de la Universidad de La Rioja.

4. Vamos a ver ahora cómo podemos configurar nuestra cuenta de correo. La Universidad nos ofrece distintas posibilidades. Una de ellas consiste en configurar el correo en nuestro ordenador personal. Para ello hay que seguir los pasos explicados en http://www.unirioja.es/servicios/si/red_servidores/correo/configuracion.shtml. También lo puedes configurar en una llave USB, tal y como se explica en http://www.unirioja.es/servicios/si/red_servidores/documentos/InstalacionThunderbirdPortable.pdf.

Nosotros nos decantaremos por la primera opción. Vamos a descargar primero el cliente de correo Mozilla Thunderbird (http://www.mozillamessaging.com/es-ES/). Lo instalamos eligiendo las opciones por defecto que el mismo ofrece.

Una vez hayamos completado el proceso de instalación, comienza el proceso de configuración de nuestra cuenta de correo. Ejecuta Mozilla Thunderbird y utiliza la opción "Crear una cuenta nueva".

Veamos las distintas cuestiones que nos plantea el programa:

- Su nombre: aquí debemos consignar el nombre que aparecerá en los mensajes que le lleguen a los demás usuarios. Como tal, puedes elegir el que consideres más adecuado;
- Dirección de correo: aquí debes especificar la dirección de correo de la cuenta que vas a configurar. En este caso, la dirección de tu cuenta de correo de la Universidad de La Rioja;
- Contraseña: contraseña de la CUASI;

Al pulsar "continuar", el programa empieza a tratar de inferir los datos de los servidores de correo entrante y saliente. Deténlo y veamos primero qué significa cada una de esas opciones.

- nombre de usuario: se refiere al nombre de tu "carpeta" en el servidor de correo. En este caso, se corresponde con el "login" de tu CUASI (como ves, por defecto, Thunderbird trataba de usar tu nombre entero);

- Entrante (Servidor de Correo Entrante): el funcionamiento del correo electrónico en un cliente distingue entre el correo entrante y el correo saliente. Ambos pertenecen a protocolos distintos dentro de la pila TCP/IP (como correo entrante tenemos POP, Post Office Protocol, e IMAP, Internet Message Acces Protocol, y como correo saliente tenemos SMTP, Simple Mail Transfer Protocol), y generalmente hacen uso de distintos servidores (y

puertos) para el envío y recepción de correos. Entre los protocolos de correo entrante, la principal diferencia entre POP e IMAP reside en que el primero descarga todos los mensajes a tu ordenador desde el servidor de correo borrándolos del mismo. De este modo, los cambios sobre los mensajes de la cuenta (borrado o lectura de mensajes) sólo tienen lugar en nuestra máquina. Es más, si nos conectamos a la cuenta desde otra máquina, en el servidor nos aparecerán sólo los mensajes que han llegado desde la última vez que nos conectamos desde la cuenta POP. Sin embargo, con el protocolo IMAP, la carpeta de correo entrante de nuestra máquina se mantiene sincronizada con nuestra carpeta de correo entrante en el servidor, de tal modo que si, por ejemplo, nos conectamos desde un segundo dispositivo por IMAP, la información entre las tres máquinas (nuestro ordenador, el servidor de correo y el tercer dispositivo) será la misma. Por tanto, como principal ventaja del protocolo POP debemos señalar que en el servidor no deja información, permitiéndonos gestionar cuentas con poca capacidad, pero su portabilidad es nula. Sin embargo IMAP ofrece gran portabilidad, pero requiere que el espacio que nuestra carpeta ocupa en el servidor pueda ser bastante grande. Configuraremos nuestro servidor de correo entrante con el protocolo IMAP. Como puedes ver en http://www.unirioja.es/servicios/si/seguridad/correoseguro.shtml#thunderbird, el nombre del servidor tanto para el protocolo IMAP como para POP será "pop.unirioja.es". Como puerto para la configuración usaremos el 993, y como nivel de seguridad usaremos el (protocolo) SSL/TLS;

- Saliente (Servidor de Correo Saliente): como protocolo de correo saliente usaremos SMTP (Simple Mail Transfer Protocol). Como los anteriores es un protocolo de la capa de aplicación. En este caso, está configurado en un servidor distinto al servidor POP e IMAP cuyo nombre es "smtp.unirioja.es" (observa que la diversificación de protocolos y máquinas podría dar lugar a situaciones en las que pudieras mandar correo y no recibirlo, o viceversa). Como puerto debes elegir el 587, y como protocolo de seguridad STARTTLS.

Con las opciones elegidas el proceso de configuración de la cuenta de correo debería estar completado.

Vete ahora a tu "Bandeja de Entrada" y trata de recibir todo el correo que tengas en tu carpeta del servidor (ten en cuenta que si tienes tu cuenta de correo redirigida a otra cuenta, la carpeta del servidor pop.unirioja.es podría estar vacía).

5. Vamos ahora a acceder a nuestra cuenta de correo desde el navegador (correo web). En realidad, lo que hace el correo web es presentarnos una interfaz de nuestra cuenta de correo que está configurada internamente por medio de imap y smtp. Abre la dirección http://www.unirioja.es/correo/index.shtml, accede con tu cuasi y envía un correo electrónico a uno de tus compañeros de clase. Comprueba lo que ha pasado en Thunderbird.

6. Elimina el mensaje que hayas recibido desde Thunderbird. Observa lo que sucede en el correo web.

Veamos ahora algunas características adicionales del servicio de correo de la Universidad.

En http://www.unirioja.es/servicios/si/red_servidores/correo/buzon.shtml puedes ver información sobre el tamaño de la cuenta de correo. Como máximo el mismo será de 500 MB. Puedes comprobar el tamaño también en www.unirioja.es/ldap.

Veamos ahora cómo podemos sincronizar tu cliente de correo con el servicio de directorio de la Universidad de La Rioja (puedes observar en http://www.unirioja.es/servicios/si/red_servidores/correo/integracion.shtml la configuración del mismo).

En el menú de "Herramientas", en "Opciones", si entras en el menú de "Redacción", pestaña "Destinatario", pulsa la opción "Servidor de Directorio". Pulsa la opción "Editar directorios", y en la misma, en "Añadir", introduce el nombre que quieras (por ejemplo "LDAP"), en servidor introduce "ldap.unirioja.es" y en la casilla "DN base" añade las opciones "o=unirioja.es,dc=unirioja,dc=es". Al salir elígelo como "Servidor de directorio".

Ahora crea un nuevo mensaje de correo y vete a la pestaña de "Para:". Comprueba si salen las direcciones del servicio de directorio de la Universidad.

7. Asegúrate de que Wireshark está capturando los paquetes en tu equipo. Crea un mensaje en Mozilla Thunderbird y mándalo a la dirección de correo de la Universidad (…@alum.unirioja.es) de alguno de tus compañeros. Comprueba que el mismo ha llegado (o al menos que Thunderbird no ha dado ningún problema al enviarlo).

8. Filtra en Wireshark todos los paquetes que han sido producidos del protocolo ldap. "Filter: ldap". Responde en tu informe de prácticas ¿Es visible la información que envían y reciben los mismos? ¿Está codificada? ¿Qué protocolo de la capa de transporte utiliza LDAP? ¿Qué puertos ("src" y "dst") ha utilizado la comunicación? ¿Qué IP tiene el servidor ldap de la Universidad?

9. Filtra ahora todos los paquetes SMTP con Wireshark ("Filter: smtp"). Captura uno cualquiera de ellos, pulsa el botón derecho, y elige la opción "Follow TCP Stream". Observa los mensajes que ha producido un envío cualquiera de correo. Responde en tu informe de prácticas ¿Qué protocolo de la capa de transporte utiliza SMTP? ¿Qué protocolos aparecen en el "Stream"? ¿Son protocolos encriptados? ¿Puedes recuperar la información de los mensajes que has mandado a través de los paquetes?

Anota en tu mensaje de prácticas los puertos que han usado los mensajes SMTP, así como las IPs de las máquinas de origen y destino de los mismos.

10. Sube el informe de la práctica a belenus y enlázalo desde tu página "index.htm".