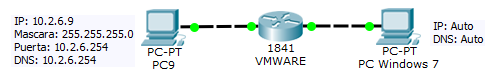
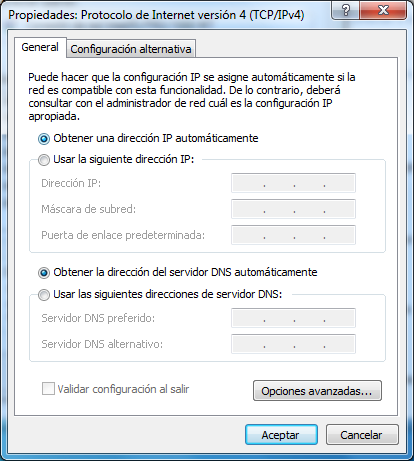
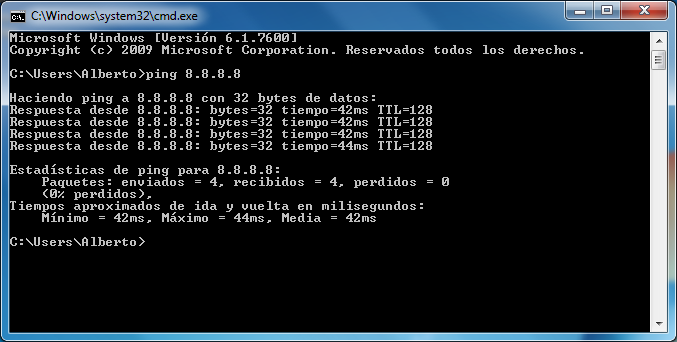
1. Esquema de la red

En la siguiente imagen podemos ver el esquema de la red que necesitamos para realizar la siguiente práctica. Como podemos comprobar tenemos un equipo físico que es nuestro equipo de clase, después podemos ver el router virtual que nos genera el programa VMWare y después podemos ver la máquina virtual que tenemos instalado en el VMWare con sistema operativo Windows 7. En la imagen podemos comprobar la configuración aplicada a los equipos con las direcciones de red aplicadas.



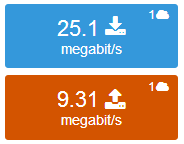
Como podemos comprobar el equipo virtual que tenemos en VMWare le hemos configurado la red de forma automática para que reciba la ip por el protocolo DHCP.

Comprobamos que con la configuración realizada tenemos acceso a internet realizando un ping a la dirección 8.8.8.8.

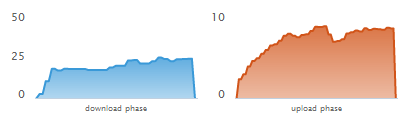


Capa 1: Física

Realizamos un test a través de la página web dslreports de la red que tenemos configurada en la máquina virtual, con ello podemos comprobar como circulan las bits por dicha red.

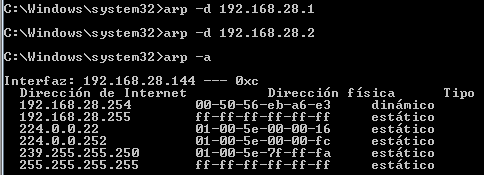
Como podemos comprobar en esta imagen tenemos una velocidad de descarga media de 25.1megabit/s y una velocidad de subida media de 9.31megabit/s.

En esta otra imagen podemos ver 2 gráficas de los niveles de la red durante el test. Como se puede ver la conexión de descarga ha sido muy buena ya que ha mantenido un nivel estable y la subida también ha sido bastante buena dado que también ha mantenido un nivel estable aunque no tanto como la descarga.

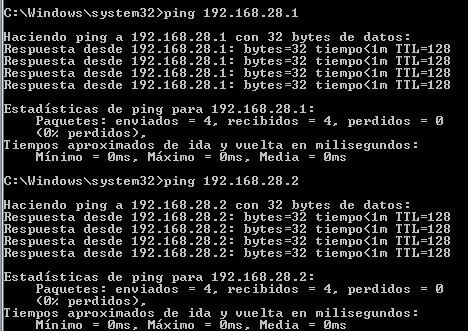


Capa 2: Enlace de datos.

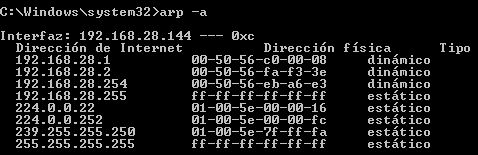
Ahora vamos la capa de enlace de datos. Para ello vamos eliminar dos direcciones de red que contenía nuestra tabla de arp donde se guardan las direcciones de red junto con la correspondiente MAC del interface.



Ahora realizamos un ping a las 2 direcciones que habíamos borrado anteriormente y comprobamos que recibimos respuesta de ambas.



Volvemos a mostrar la tabla de arp con el comando que vemos en la imagen y comprobamos como nos ha agregado estas 2 direcciones a la tabla.



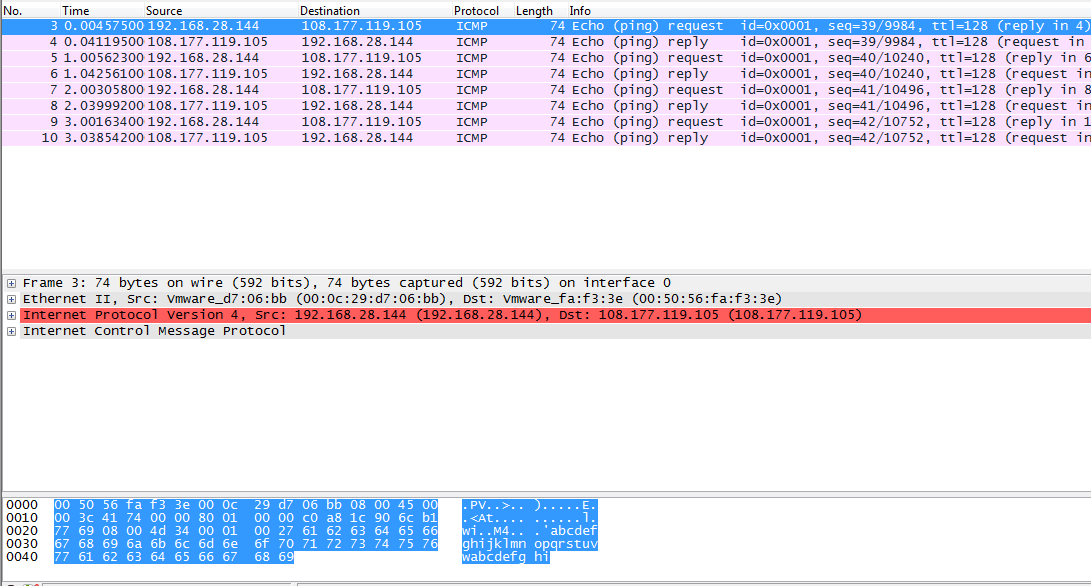
Como podemos ver en esta imagen de la configuración total de la red la dirección 192.168.28.2 corresponde a la puerta de enlace de nuestro router virtual de VMWare. La dirección 192.168.28.1 corresponde a la dirección que da VMWare para comunicar con la red física.



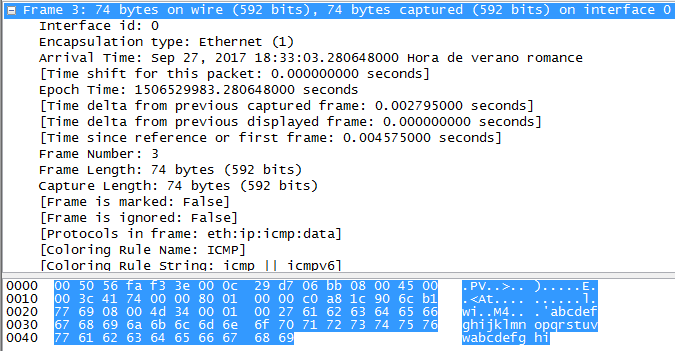
Capa 3: nivel de red.

Ahora vamos a utilizar el programa wireshark para comprobar los datos que se envían cuando realizamos ping a entre dos equipos. En ellos veremos las diferentes capas llegando a la capa 3 y que podemos ver en cada una de ellas.

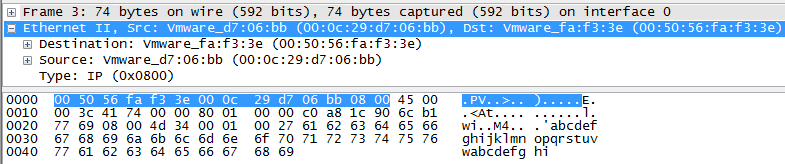
En esta imagen podemos ver los pings que hemos realizado desde nuestro equipo a la dirección de google y podemos ver por cada envío recibimos una respuesta.



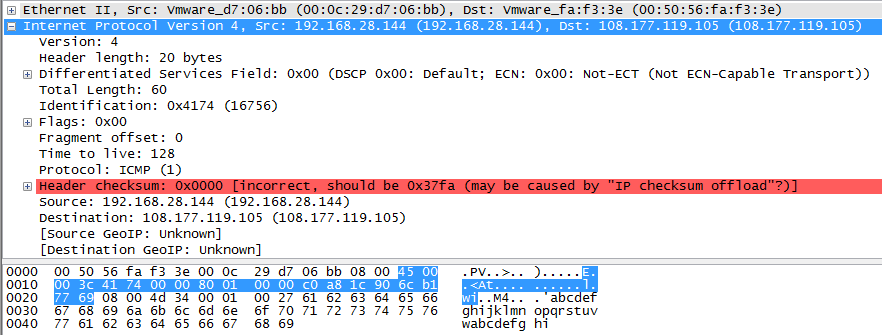
Ahora vamos a ver los datos que se muestran en cada capa, el frame es la capa 1 donde están todos los datos en bits, podemos ver que el tamaño del paquete es de 74bytes que en la parte de abajo están representados en varias líneas con código hexadecimal. Además también podemos ver la fecha y hora del envío de paquete.



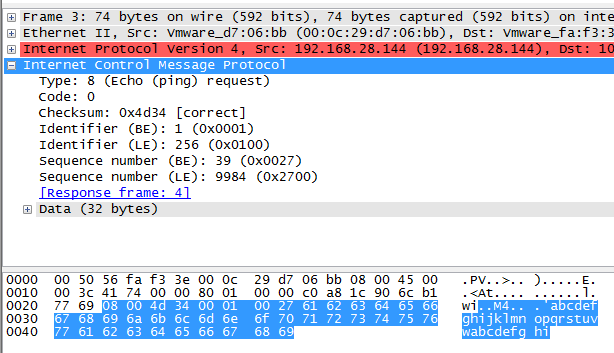
En esta otra imagen vemos la capa 2 donde podemos ver las direcciones MAC tanto de envío correspondiente a nuestra interfaz de red como la de recepción del interfaz de nuestro router virtual. Al seleccionar la capa podemos ver que en la parte de abajo nos destaca la parte de bytes que corresponden a esta capa.



En la última capa vamos a ver los datos que se ven en la capa 3, donde podemos observar las direcciones de red tanto del emisor que somos nosotros como la dirección ip del receptor, en este caso [www.google.com](http://www.google.como), aunque nos muestra la dirección ip del mismo. Al igual que en la anterior imagen en esta podemos comprobar la parte de bytes que corresponde a la capa de red. Podemos ver que tiene un tamaño de 20bytes y 128 saltos de vida.



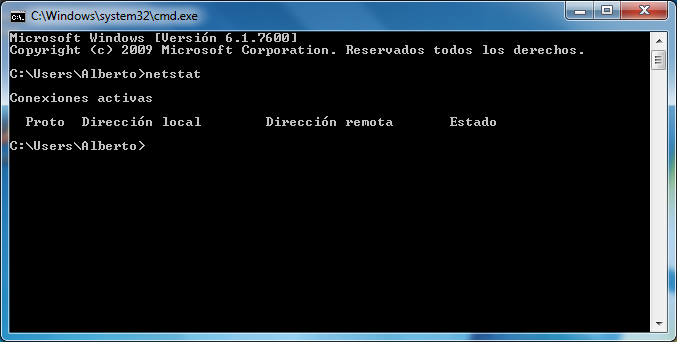
Por ultimo vemos la parte que corresponde al ICMP que envía para realizar ping. Podemos comprobar en la parte de abajo la cantidad de bytes que corresponden al mensaje total que se envía. Comprobamos que envía un checksum, para comprobar que el mensaje es correcto.



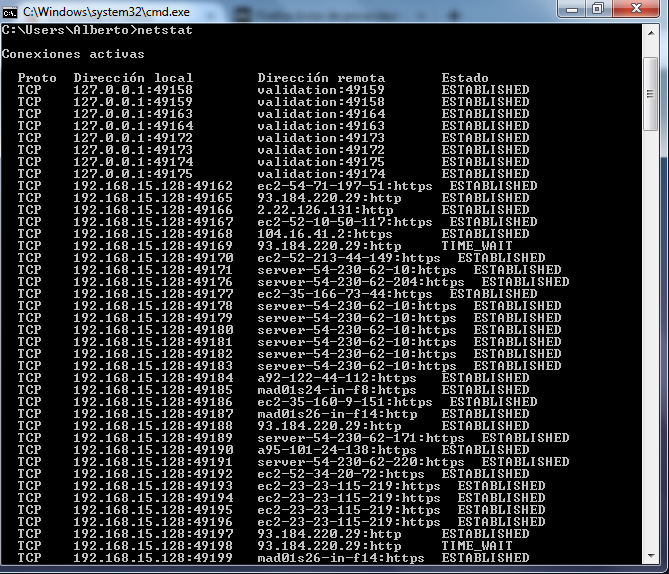
Capa 4: Transporte.

Vamos a comprobar la capa de transporte que utiliza los protocolos UDP o TCP.

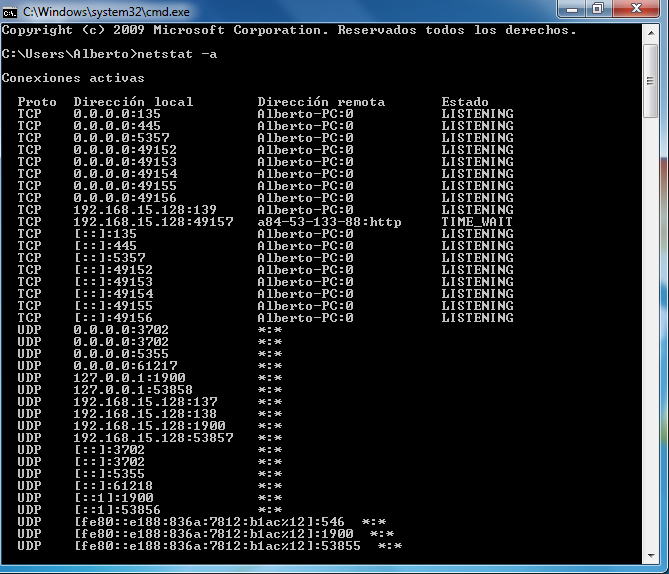
Como podemos ver en la siguiente imagen una vez arrancamos el equipo y realizamos un netstat comprobamos que aún no se ha producido ninguna comunicación.



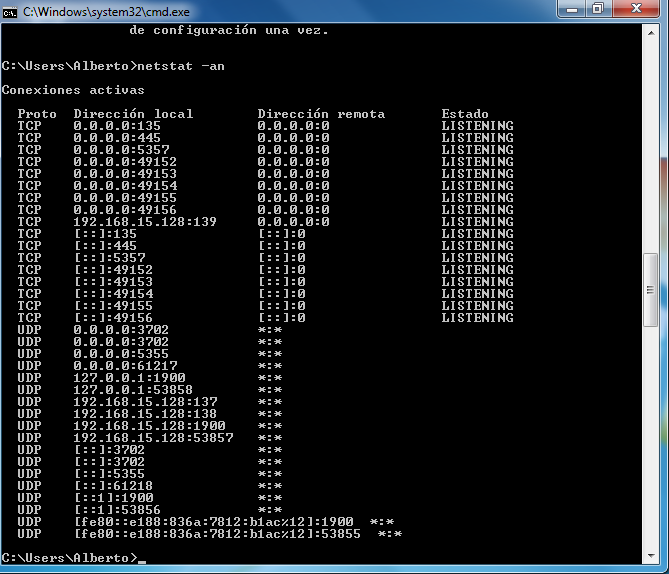
Una vez iniciamos sesión con el navegador podemos comprobar que comienzan a producirse comunicaciones por TCP, las primeras son seguramente de comprobación de funcionamiento y después comunicación con diferentes host para la descarga de las páginas web que visitamos. En la columna de la izquierda podemos observar el protocolo usado de la capa de transporte y en la siguiente columna podemos ver nuestra dirección y el puerto por el cual está trabajando. En la columna de dirección remota podemos observar la dirección y el protocolo como se conecta, si esta siento HTTPS o HTTP y en la columna de la derecha podemos ver el estado de esa comunicación.



Si nada más encender nuestro equipo realizamos un netstat –a podemos visualizar no solo las conexiones activas, sino que nos mostrara todas las conexiones que en este momento no están activas dado que un equipo nada más encender ya se está comunicando con la red aunque no tenga ninguna conexión establecida.



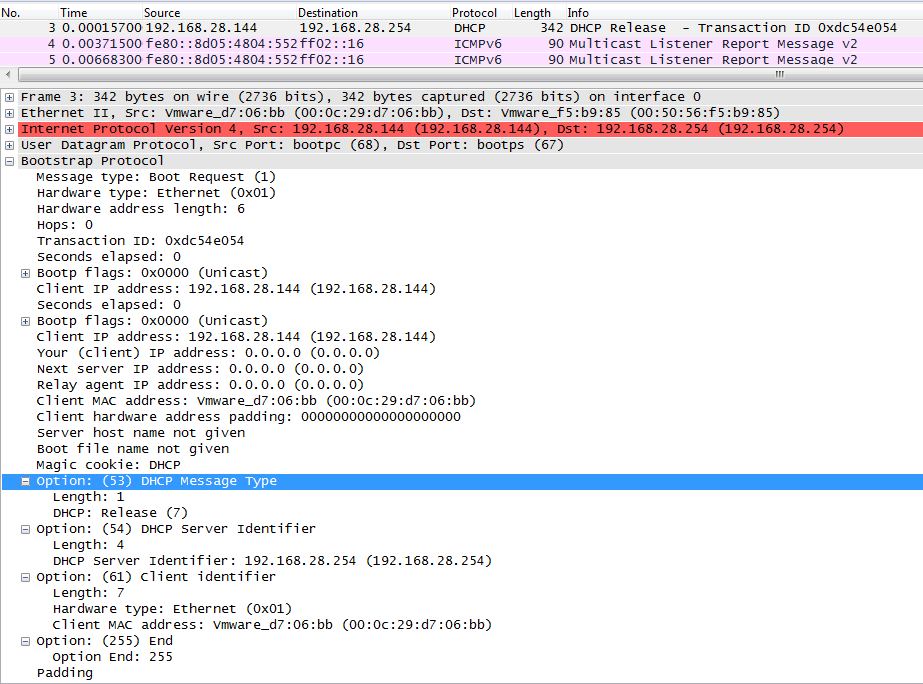
El comando netstat –an no muestra los mismos datos solo que en este caso todos los datos de puerto, host y toda la comunicación los muestra en formato numérico.



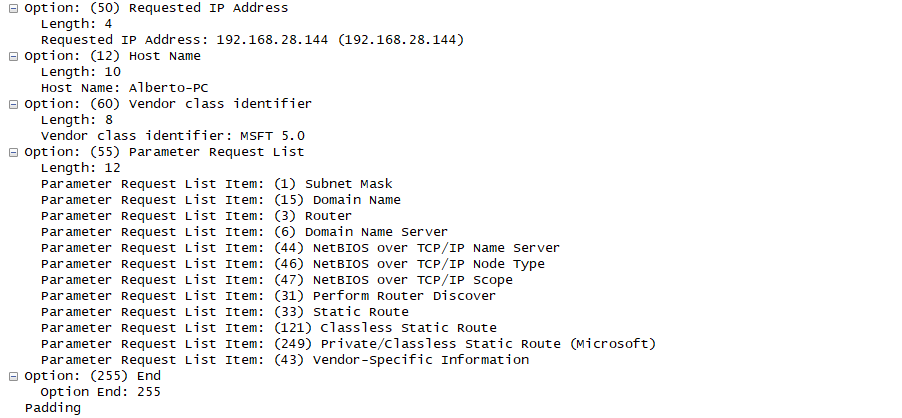
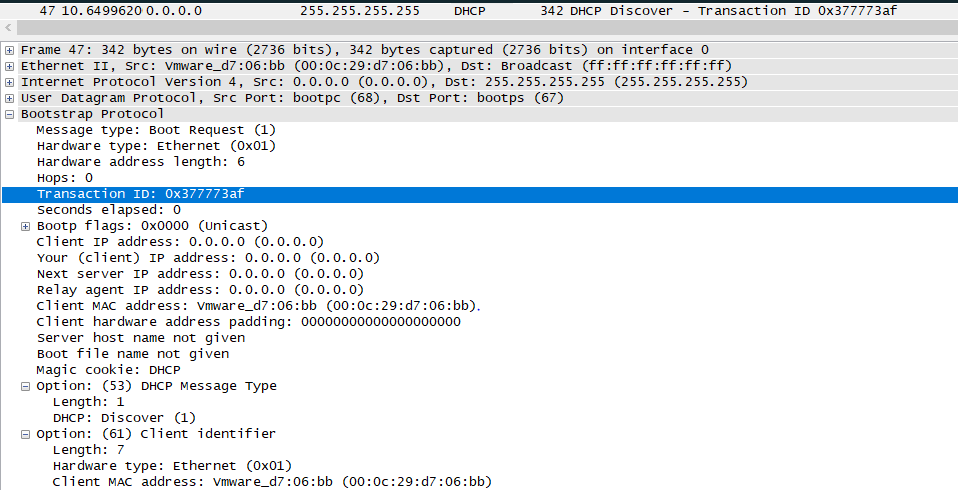
Capa 5: Sesión.

Vamos a realizar la eliminación del DHCP y volver a reclamarlos por parte del cliente.

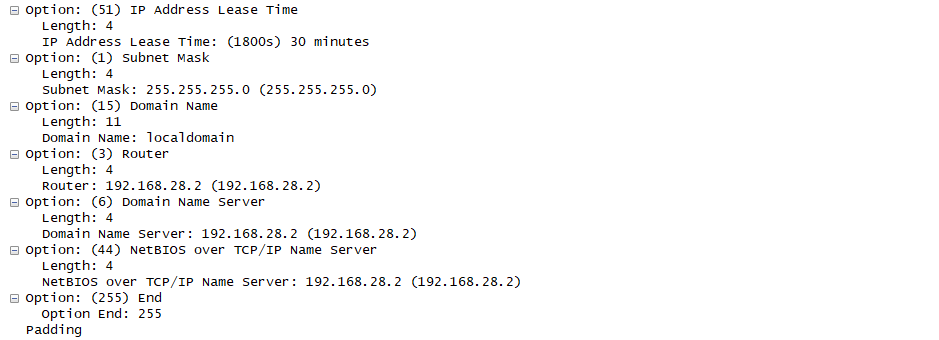
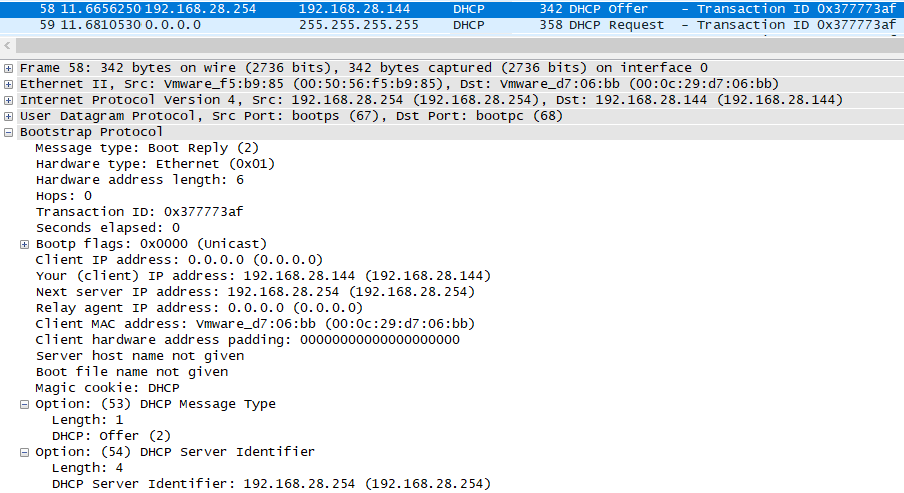
Como vemos en la imagen primero hacemos un DHCP reléase con el cual el cliente indica al servidor de DHCP que ya no va a utilizar esta dirección ip que tenía asignada. En la imagen podemos comprobar que estamos trabajando en capa 5 de sesión como nos indica el protocolo bootstrap. Si nos fijamos en los diferentes apartados podemos ver que el cliente le está indicando la dirección ip que utilizaba, la MAC de su interfaz y se ve la ip del servidor de DHCP al que se lo envía.



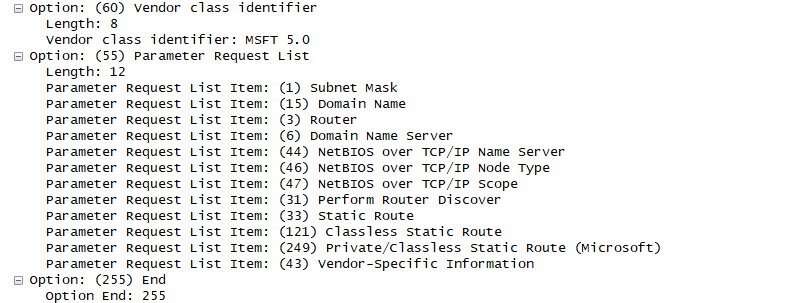
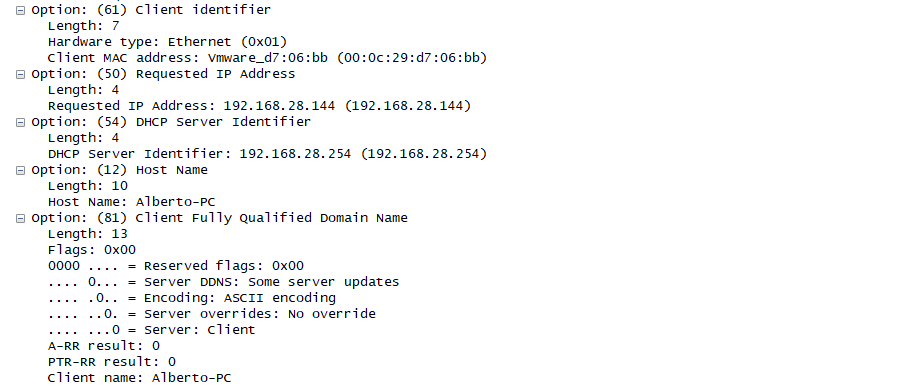
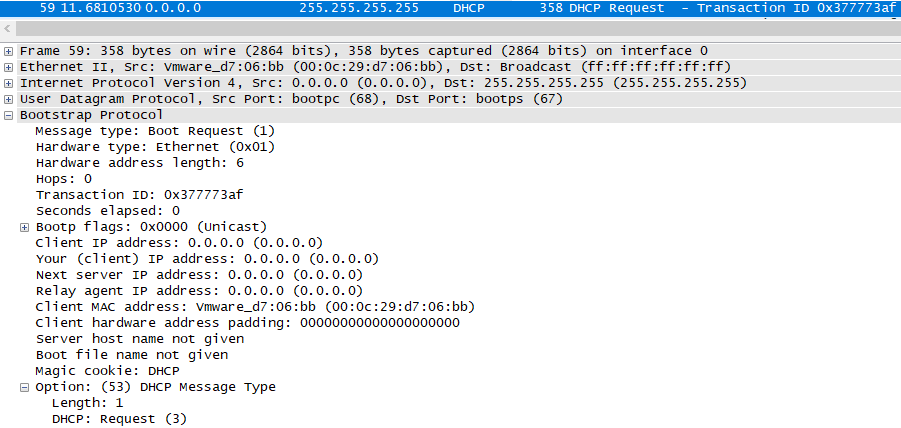
Ahora vamos a pedir por parte del cliente una ip DHCP, para ello lo primero el cliente envía la señal discover para averiguar los servidores DHCP que hay. Como podemos comprobar el equipo envía en el mensaje su dirección MAC y los datos de IP los envía en blanco dado que no los tiene. Podemos ver un apartado con los parámetros que reclama para configurar el protocolo DHCP, el nombre del host y el tipo de mensaje del protocolo DHCP.



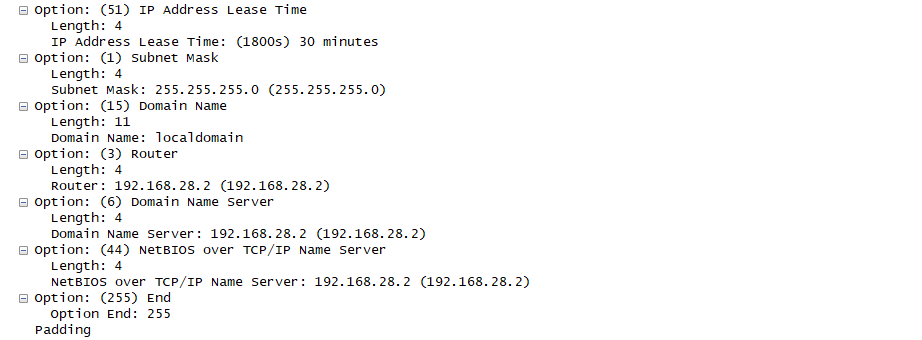
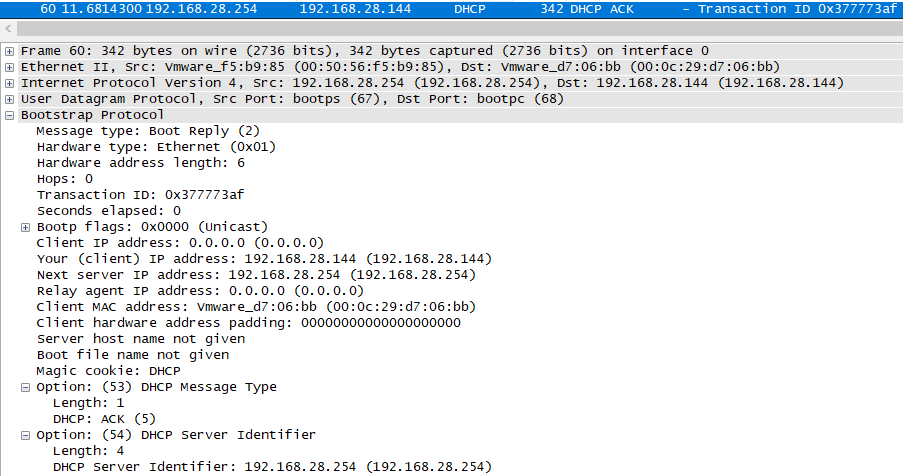
Ahora es el servidor quien contesta al cliente indicando que tiene una red disponible e indicando los parámetros de la misma, como pueden ser IP, mascara, puerta de enlace al router, nombre de dominio y el tiempo máximo de 30 minutos por el que le concede esta dirección de red.



El siguiente mensaje lo envía el cliente al servidor, en su respuesta le comunica al servidor que se queda con la dirección. Como se puede ver en la imagen sus datos de red están vacíos dado que aún no se ha configurado, él envía sus datos en blanco dado que solo está confirmando que la dirección de red proporcionada se la queda asignada para él y el servidor deberá marcarlo en su lista para no asignarlo a otro host.



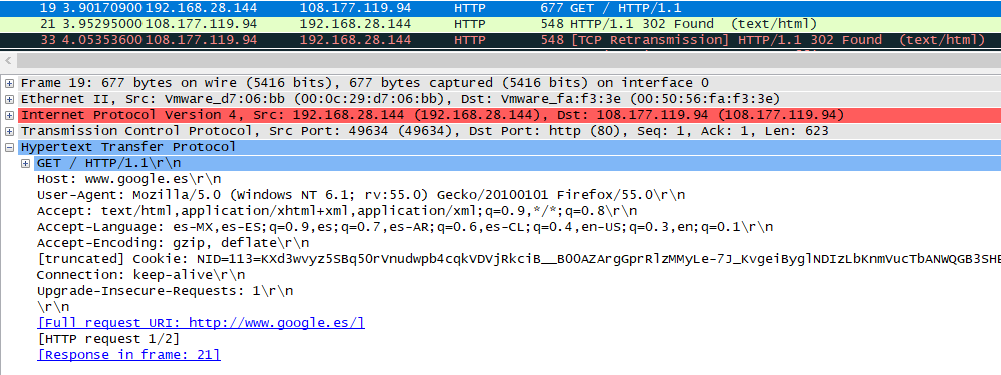
El último mensaje que se envían lo hace el servidor, en este mensaje ACK el servidor vuelve a enviar todos los datos al cliente para la configuración de su dirección de red, se puede decir que este mensaje confirma por parte del servidor al cliente que esta configuración de red la deja reservada para este host y que no proporcionara la dirección IP a otro.



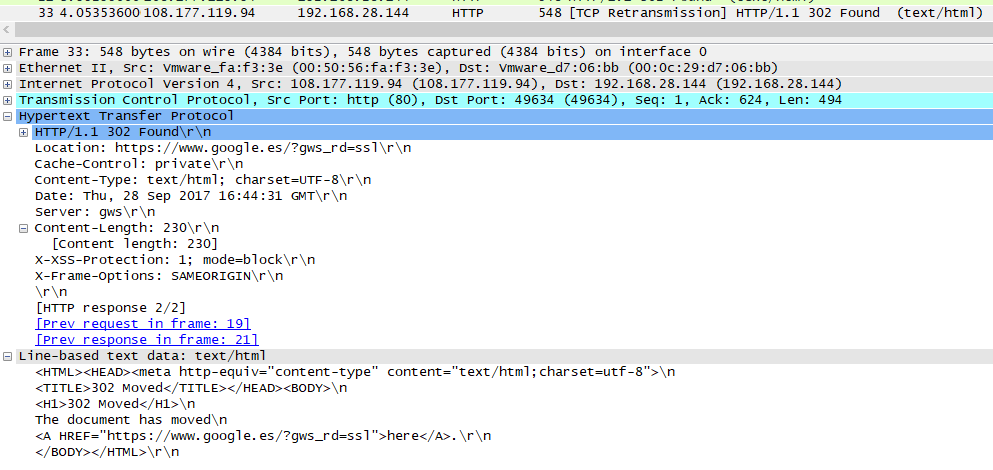
Capa 6: Presentación.

Para visualizar la capa de presentación vamos a entra en la web de google.

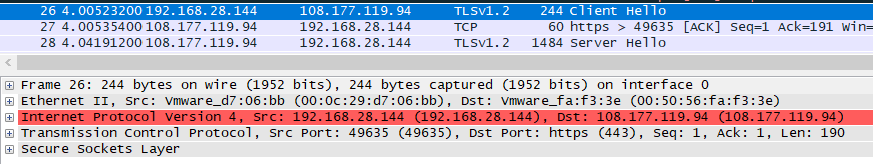
En la siguiente imagen podemos comprobar como nuestro equipo envía la petición al servidor solicitando el portal [www.google.es](http://www.google.es). En la imagen podemos ver como solicita un protocolo http y los datos de la aplicación que abrirá el protocolo con los datos de configuración.



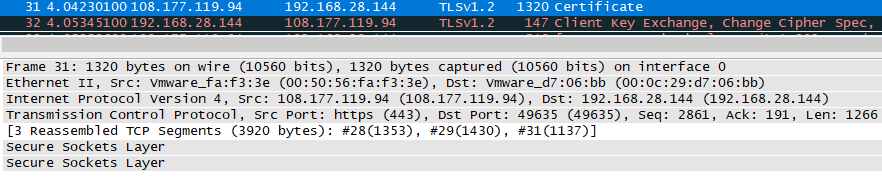
Después podemos comprobar la respuesta del servidor enviando la localización del portal web, redirigiendo a una página https y proporcionado el tipo de lenguaje usado y todos los datos necesarios para la visualización de la página en nuestro navegador.



Al comenzar una comunicación usando el protocolo https la información va encriptada, como vemos en la imagen el siguiente paquete es de saludo entre el cliente y el servidor para comenzar esa comunicación usando SSL. En la misma imagen podemos ver el paquete de respuesta del servidor al cliente con un saludo también usando SSL.



Los siguientes 2 paquetes que vemos en la imagen son de intercambio de código para que cliente y servidor puedan encriptar y desencriptar los paquetes que se envían y poder establecer una comunicación correcta.



Durante la comunicación se enviaran y recibirán mensajes del tipo TCP, estos paquetes sirven para controlar que la comunicación entre cliente y servidor es correcta. También en la imagen podemos ver paquetes TLS que son los paquetes que contienen la información de la página web, al igual que toda la información va encriptada.

