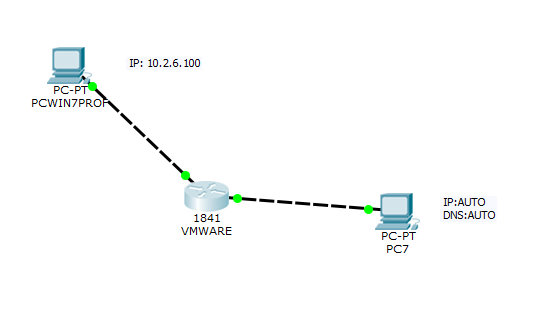
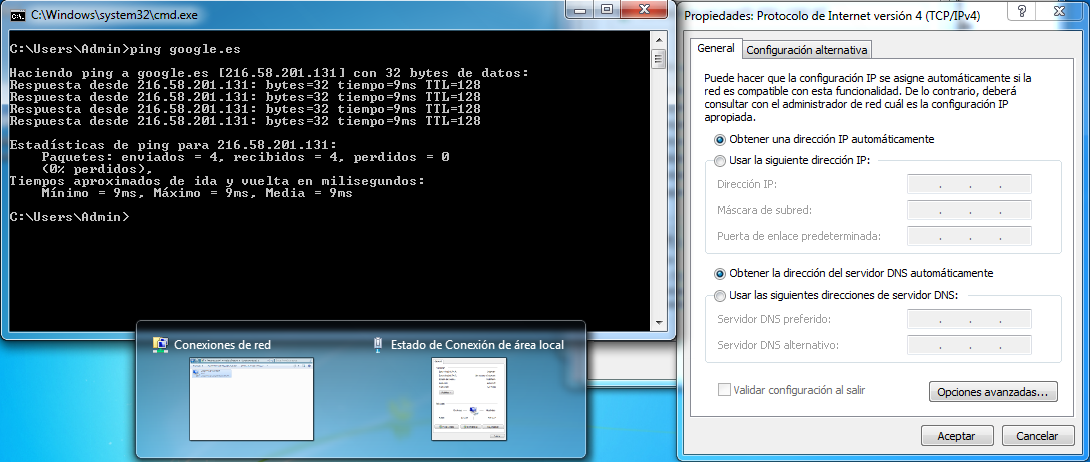
# 1.- Esquema de la red

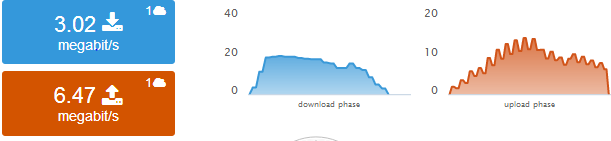


# 2.- Preparación de la máquina,

Capturas de las **configuraciones y las comprobaciones** más importantes que has realizado



Nivel físico: captura del test de velocidad y conclusiones



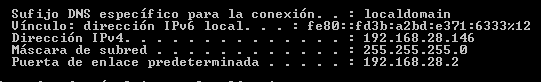
Conclusión. Si hacemos el test de velocidad mientras desde la misma red están haciendo descargas o usando el ancho de banda de internet, el test no será fiable al 100%, ya que el ancho de banda se está dividiendo.

En la gráfica se puede ver que aunque la velocidad no es muy grande, se puede decir que es más o menos estable.

Nivel enlace:

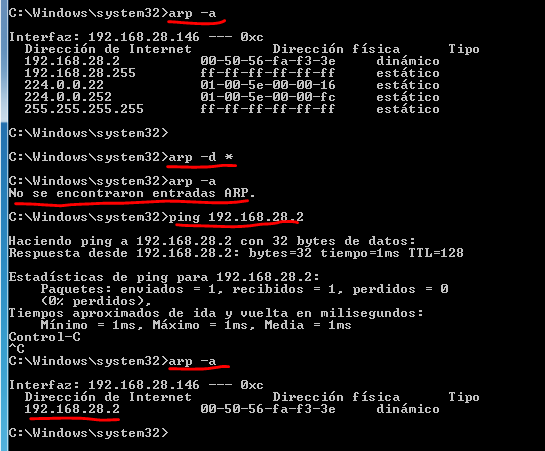
Capturas ipconfig/all





arp –a, Ping

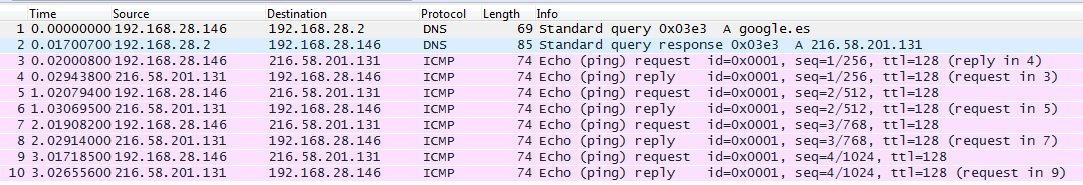
Comprobamos las entradas en la tabla arp, luego las eliminamos y volvemos a listar las entradas en dicha tabla, comprobando que no hay ninguna. Tras esto, realizamos un ping a una de las maquinas (en este caso el router) y volvemos a comprobar la tabla arp y comprobamos que se ha añadido dicha maquina a esta tabla



Nivel red: <https://www.wireshark.org/>

Capturas y explicación de ping a www.google.es, desde ICMP, IP, Ethernet hasta Frame

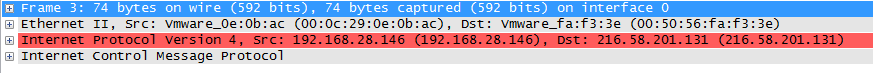
Cuando realizamos un ping a google lo primero que capturamos con wireshark es lo siguiente:



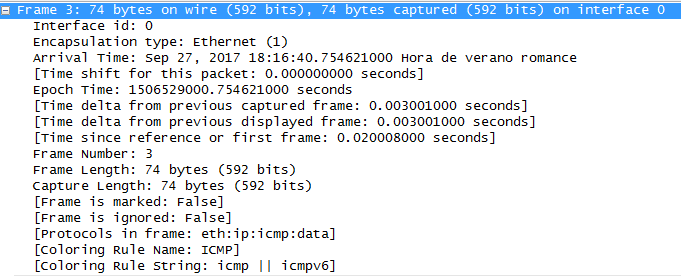
Vemos que lo primero que se realiza es una petición dns para saber cuál es la ip de google, lo podemos ver en el paquete nº1, y en el paquete n2 vemos la respuesta del servidor dns (que en este caso es el router).

Luego vemos que hay 4 parejas de petición y respuesta de icmp.

Cada petición y respuesta icmp tiene la siguiente estructura:

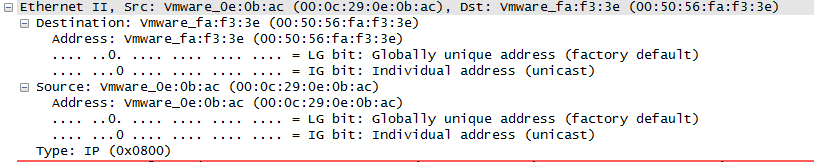


Podemos ver que tiene cuatro partes, la primera es frame que representa la capa física, si lo abrimos podemos ver los siguiente.



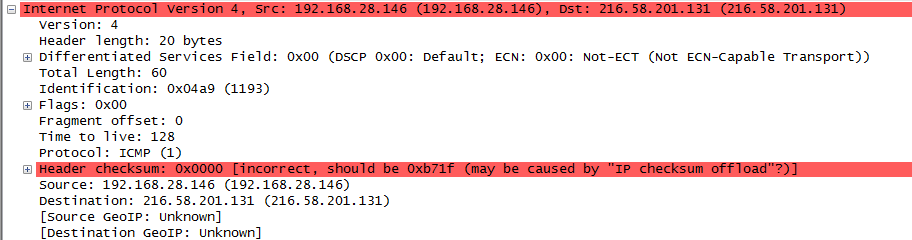
Que son las cabeceras que se han puesto en esa capa. Se pueden ver el tipo de encapsulación, la hora en la que se ha recibido, el tamaño del paquete entre otros datos.

La segunda capa que vemos es la capa enlace de datos en la que podremos ver lo siguiente:



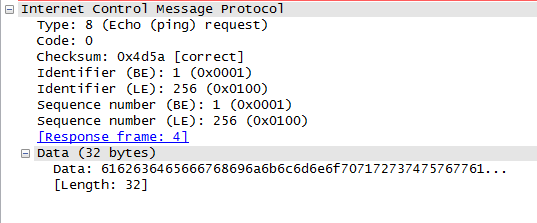
Ahí podemos comprobar las direcciones mac origen y destino así como sus respectivas banderas.

En la tercera capa, que corresponde a la capa de red vemos lo siguiente:



Podremos comprobar la información correspondiente a las direcciones ips, el protocolo (en este caso v4), las direcciones origen y destino y algún dato más.

En la última capa que nos aparece que se corresponde a la información del icmp (los datos) vemos lo siguiente:

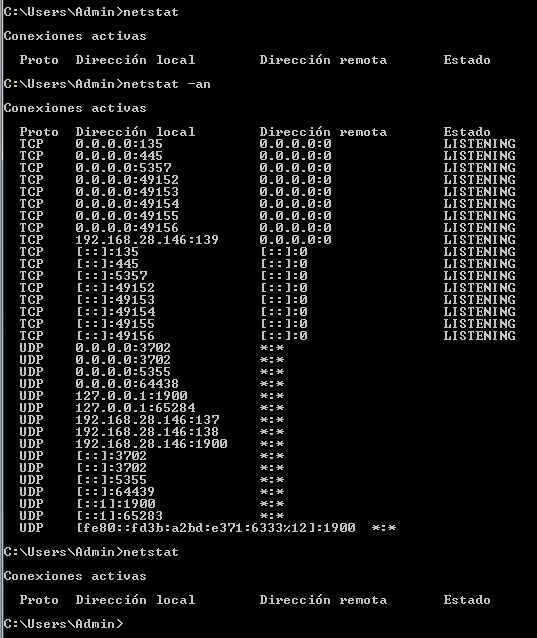


Podemos ver el tipo de mensaje icmp (8 en este caso que corresponde a una petición request), el checksum, el número de secuencia, y también vemos los datos reales del paquete en la sección DATA

## Nivel transporte: netstat -an

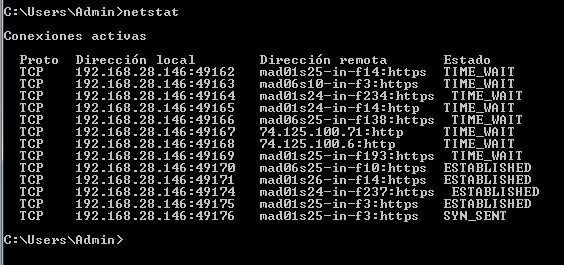
Net stat es un programa que nos permite ver las conexiones de nuestro ordenador

Como se ve en la imagen un netstat –a nos muestra todas las conexiones incluso las que están a la escucha



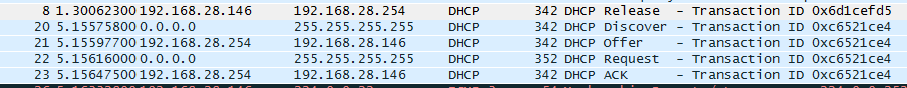
Como se puede ver en la imagen teniendo todos los programas cerrados, tenemos servicios a la escucha, como se ve al ejecutar netstat –an, pero si ejecutamos netstat a secas, no vemos ninguna conexión porque ninguna esta activa.

Si abrimos el chrome por ejemplo veremos lo siguiente:



## Nivel sesión: DHCP

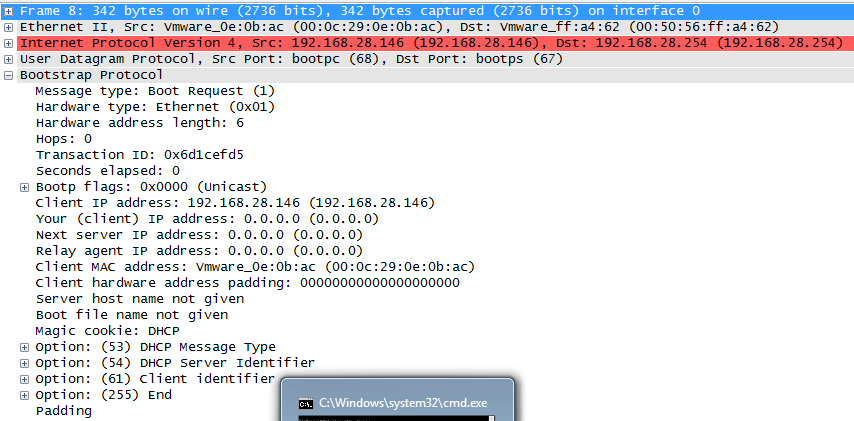
Los tipos de paquetes más importantes en dhcp son los siguientes



El primero que podemos ver, es un paquete que envía el cliente al servidor cuando un cliente quiere liberar una dirección ip, este paquete no forma parte de “la petición” de una dirección ip sino de lo contrario (liberar la ip cuando el pc se va a apagar por ejemplo)

A parte de las partes de las capas física, enlace de datos, y red, vemos una nueva parte que es la que tiene la información útil del paquete

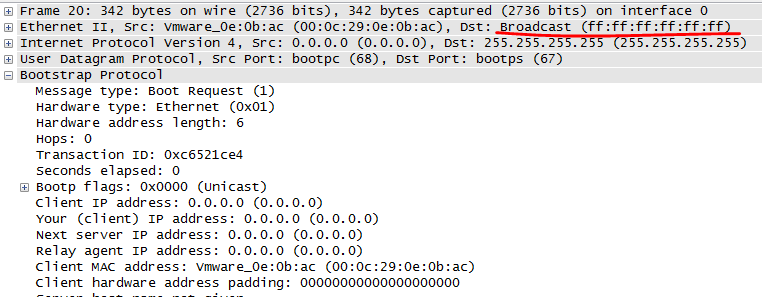




Como vemos en la imagen, vemos entre otros el tipo de mensaje, la dirección ip que teníamos (la que se va a liberar), la nueva ip que cogerá nuestro esquipo (0.0.0.0), la mac… y otras opciones.

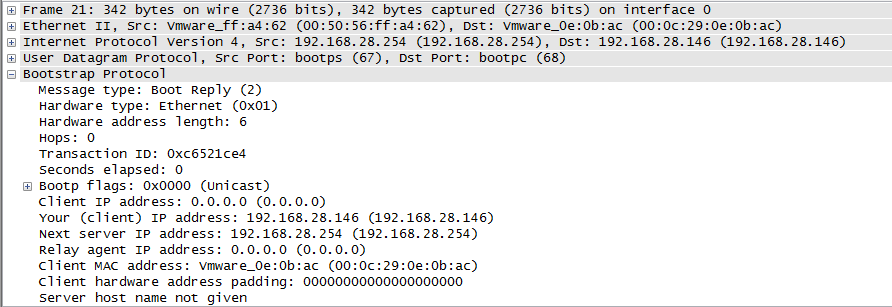
En el paquete del tipo discover, como en ese momento el equipo que quiere solicitar la dirección ip todavía no tiene una dirección, ni sabe si hay, y en tal caso quien es el servidor dhcp este paquete se manda por broadcast como se puede ver en la siguiente imagen, también podemos ver que es del tipo 1





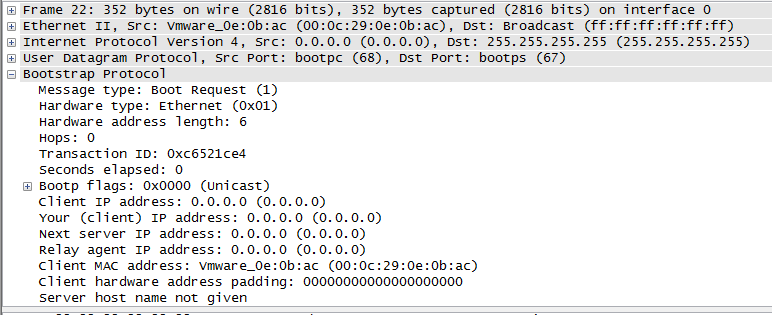
Cuando el servidor recibe el paquete el servidor manda un paquete offer diciéndole una dirección ip que tiene libre el servidor, y espera a que el cliente confirme que se queda la dirección





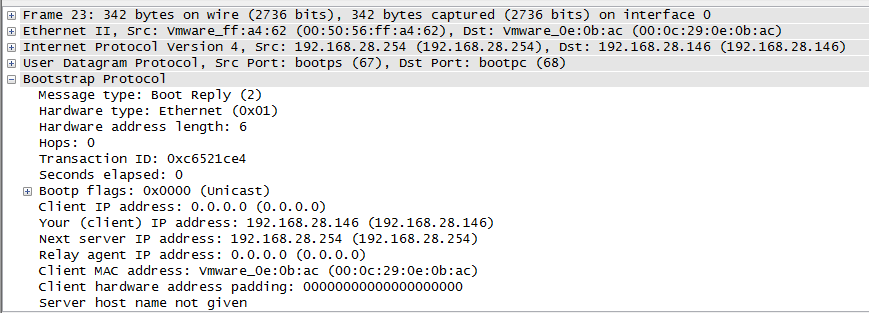
En ese momento, el cliente que ha recibido el paquete offer, manda un paquete request a servidor, solicitándole esa dirección ip.



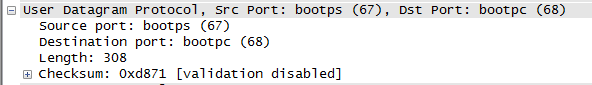


En ese momento, el servidor le manda al cliente un paquete ack confirmándole al cliente que la dirección ha sido reservada para el



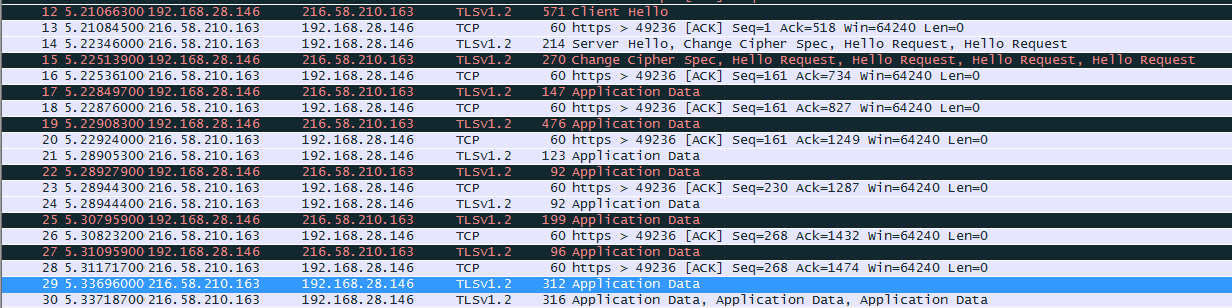


Todos estos paquetes de dhcp usan el protocolo UDP como se puede ver en la siguiente imagen, usando los puertos 67 y 68

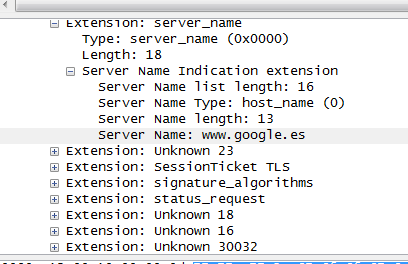


Nivel presentación: usar wireshark para analizar  el tráfico generado al abrir en el navegador [www.google.es](http://www.google.es)

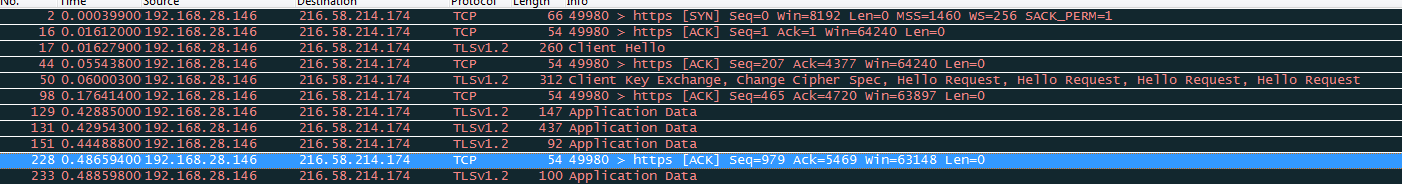
Si realizamos una búsqueda en google, vemos los paquetes en wireshark pero como google funciona con https vemos que todos los paquetes tienen el contenido cifrado



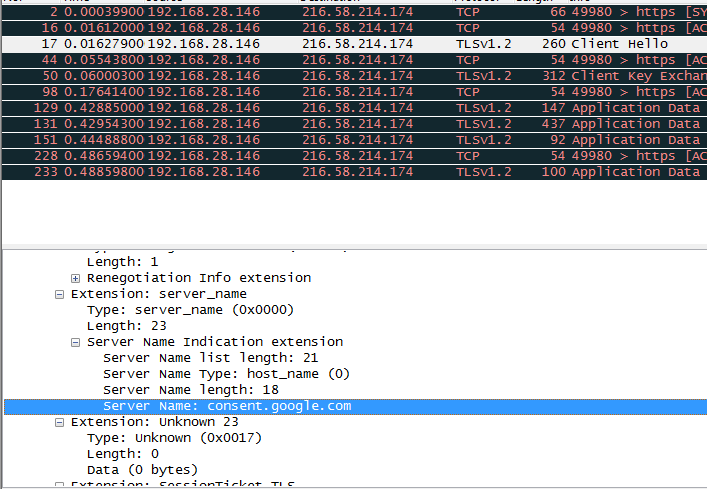
Aunque mirando por las cabeceras de los paquetes podemos ver a qué dirección se está haciendo la consulta



Si miramos los paquetes que van hacia google (donde debería estar la consulta “asereje”) vemos lo siguiente



En el paquete helo podemos ver el dominio google



En los paquetes recibidos con origen (ip de google) vemos también el dominio, el certificado digital pero no podemos ver la palabra de búsqueda ni ningún otro dato

