**Tema 1 – DHCP**

DHCP → Dynamic host configuracion protocol → un protocolo para configurar host automáticamente.

Cuando un equipo está en una red necesita tener una ip, podemos hacerlo todo manualmente, pero podemos automatizarlo mediante un DHCP.

Esto es la leche para configurar cosas.

Ahora, cuando yo quiero ofrecer un servicio web, tener una IP dinámica no mola porque no puede gestionarse bien, si yo monto mi web, y mi ip pública del router es X, cuando mi amigo se conecte, la primera vez funciona, ahora mañana será otra, y yo no cambio la ip del dominio, no puede entrar.

Esto se solucionaría con 2 cosas, estableciendo una ip estática (a pagar) o usar cosas como dyndns o no-ip.

Esto son programas que lo que hacen es analizar tu ip publica y anotarla, si el DHCP te cambia la IP, se da cuenta del cambio y configura tu dominio automáticamente a esa nueva IP.

Cuando mi router de ip publica recibe peticiones web lo que hace es redirigimiento de puertos, esa petición me la manda a mi PC con mi IP por el puerto 80.

¿Como funciona DHCP en una red?

Primero tenemos que distinguir DHCP cliente y DHCP server, el servidor es quien proporciona el funcionamiento DHCP a toda la red, y el cliente es el programita que se encarga de comunicarse con ese servidor para solicitar la IP.

Vamos a hacer ejemplito con packet tracer.

1º: El cliente manda una trama broadcast a la red con un DHCP DISCOVER, esta trama lo que busca es un servidor DHCP en la red. Para ello manda un discover a toda la red, es decir, broadcast.

Como el pc esta limpito, no tiene ip, esta trama se manda con IP origen 0,0,0,0: 68, y es una trama de tipo UDP. Se utiliza UDP porque vamos a hacer una solicitud muy breve, rápida y ligera, es decir, no merece la pena establecer una comunicación TCP por todo el proceso lento.

El destino de esta trama será broadcast es decir 255,255,255,255:67

Si el CLIENTE manda un discover y no obtiene respuestas, se repite todo el proceso y vuelve a solicitar un DHCP.

2º: Dentro de la red, todos los servidores DHCP escucharan ese discover, y por tanto, ofrecerán su servicio al cliente, es decir, cada uno de ellos mandará una trama DHCP offer, en esta trama le dan todo lo necesario, pues su ip, su mascara, dns, etc. Si solo hay un server, pues solo habrá 1 oferta.

3º: El cliente elige una de las ofertas, o coge la que es única si es única, y esa elección debe ser comunicada a los servidores, así como a los otros clientes de la red (aunque estos descartan la trama porque no va con ellos el asunto). Por tanto, se manda una nueva trama, DHCP Request, también de tipo broadcast.

En esta trama se especifica la ID del DHCP que ha sido elegida. DE esta forma, el DHCP sabe que ha sido elegido.

4º: Se produce una trama DHCPACK (un paquete ack, acknowlogment, es decir, acuse de recibo), es decir, el servidor dice que recibido y que muchas gracias por elegir mi servicio.

Así que ahora con la teoría, vamos a hacer una práctica con máquinas virtuales, concretamente vamos a instalar un servidor DHCP, concretamente ISC (tenemos link con los pasos en el aula)

Practica con 2 máquinas:

1º instalamos el servicio

OJO, ahora tenemos que quitar el modo NAT de la maquina y ponernos en red interna o no furula

2º configuramos la tarjeta-elegir cual vamos a usar básicamente

3º configuramos el archivo de config con el rango de la red que queremos y la propia red

4º nos asignamos en la máquina que hace de servidor una IP ESTATICA de esa red

NOTA: Aquí lo primero, comprobar que tu IP no está en modo automático.

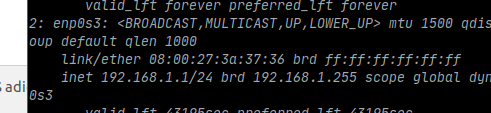
NOTA2: Comprobar que la IP está bien puesta con ip a s /ipconfig, si está bien puesta, nos debería salir la ip, y si no está bien puesta, desconectamos el cable de red y lo conectamos, para que se actualice.

5º hacemos el enable servicio, start servicio y status servicio. Si esta verde, estamos guay.

6º conectaos con otra máquina virtual, TAMBIEN EN RED INTERNA, y le hacemos un ip a s o un ipconfig /renew si es windows, y deberíamos tener una IP

Esto es en el server

Esto es en el cliente

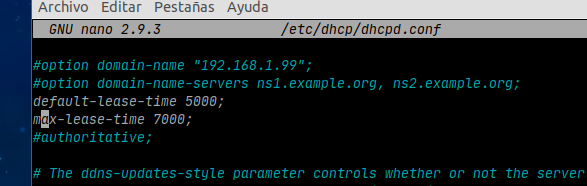


Hoy vamos a proseguir un poco con el servidor dhcp de ayer.

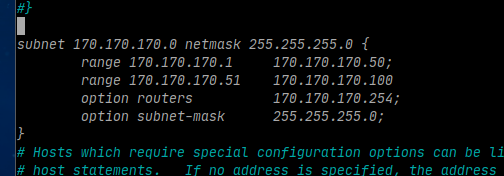
Vamos a probar diferentes rangos de ips, lo que se llama lease o leasing en inglés, algo como préstamo de ips, y el dns.

Luego lo subimos al github. Hoy voy a intentar hacer fotitos, que ayer no hice, y las ha pedido.

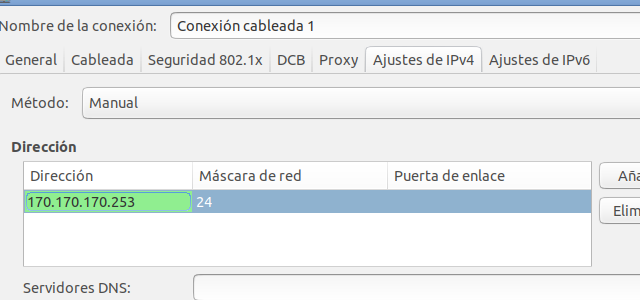
Aquí tenemos cambiado el LEASE time (era 3000 no sé cuántos y 8000 o algo así, además estaba comentado)



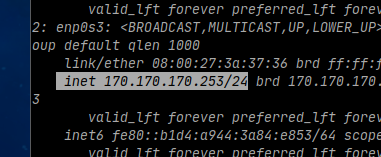
Aquí cambio el rango de Ips, ayer tenía solo 1 rango, y era en la 192,168,1,0



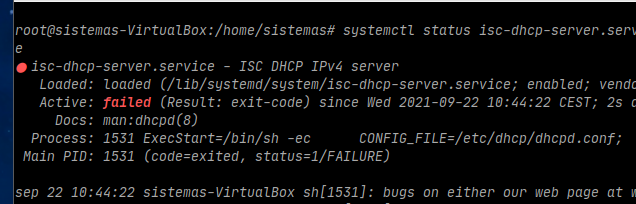
Cambio la IP del servidor



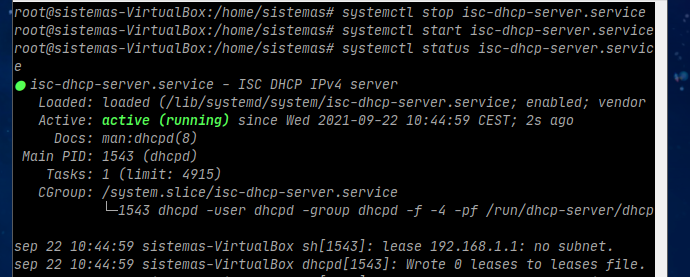
Y compruebo que se ha cambiado



RECUERDA poner las malditas ; y } en el doc de confi, que si no te pasan estas cosas

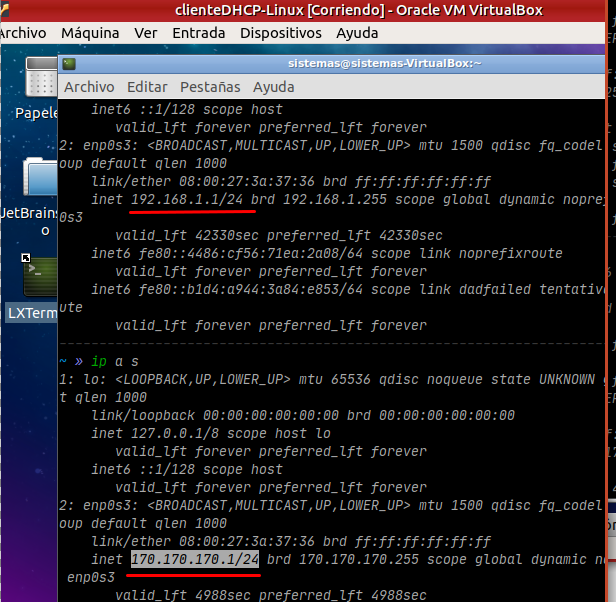


Ale, solucionado



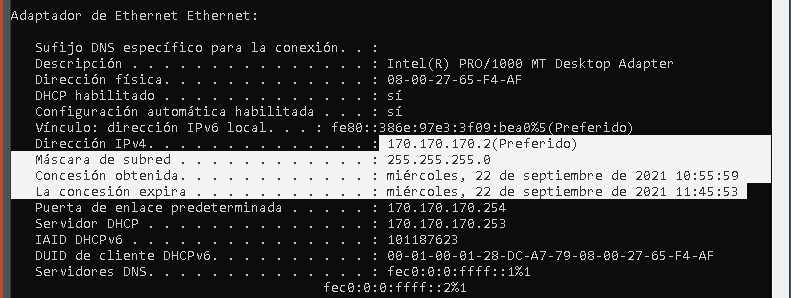
Nos vamos al cliente

Estábamos en la red anterior, guardamos los cambios, y solicitamos la nueva ip. Ahora lo mismo, pero en windows bonito.

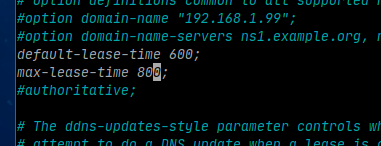


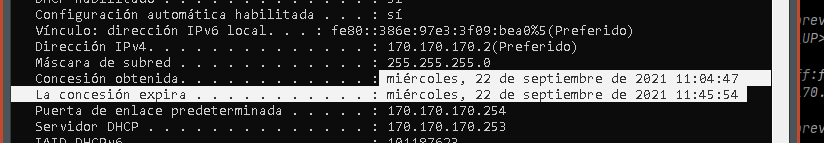
En el

windows me ha dado la dirección 2, porque la 1 esta cogida ahora mismo por el linux, y como tengo puesto 3000 de LEASE time, que son 50 minutos, pues la concesión me dura 50 minutos.



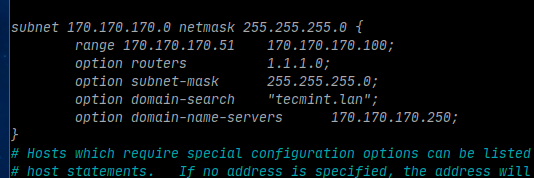
Voy a bajarlo a 600 y hacer un renew, a ver qué pasa. /RELEASE para lliberarte y /renew para pillar otra nueva, mas eficaz que solo renew.



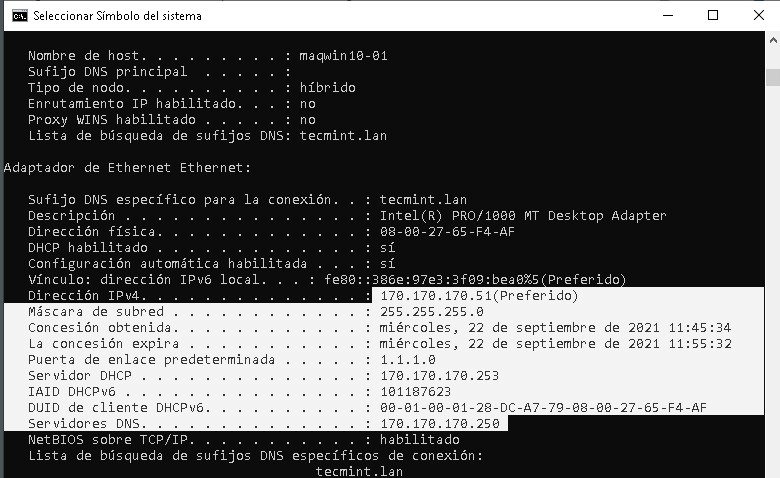


La IP NO CAMBIA, pero si me ha cambiado el tiempo de concesión, aunque son 40 minutos, y en teoría el máximo son 13. Explicación a posteriori: Entre que son máquinas virtuales y fallan un poco, y que lo hice mal para conseguir el /renew, pues pasan cosas, cambiar el lease funciona, haz primero el /reléase y luego el /renew o no se aplican correctamente.

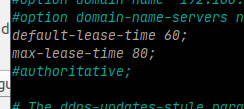
Como quiere 3 cambios, pues vamos a cambiar cosas: Quito uno de los rangos, ahora tiene que darme una ip diferente, le he puesto un router diferente, y le he puesto DNS, a ver qué pasa. Esto lo tengo en un documento aparte, mejor explicado.

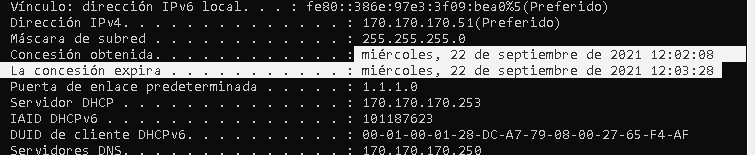


aquí podemos ver que tenemos el servidor DNS 250, el router es el 1,1,1,0, y que la IP es del rango 50-100. Y abajo del todo sale también el DNS especifico. Buen trabajo chicos, ha funcionado.



En el windows, cuando queramos hacer cambios de ips y cosas para comprobar, haz primero un ipconfig /release y luego el /renew, es decir, abandonas tu ip, y pides una nueva, en lugar de estar haciendo movidas de cambiar la red o reiniciar el pc.



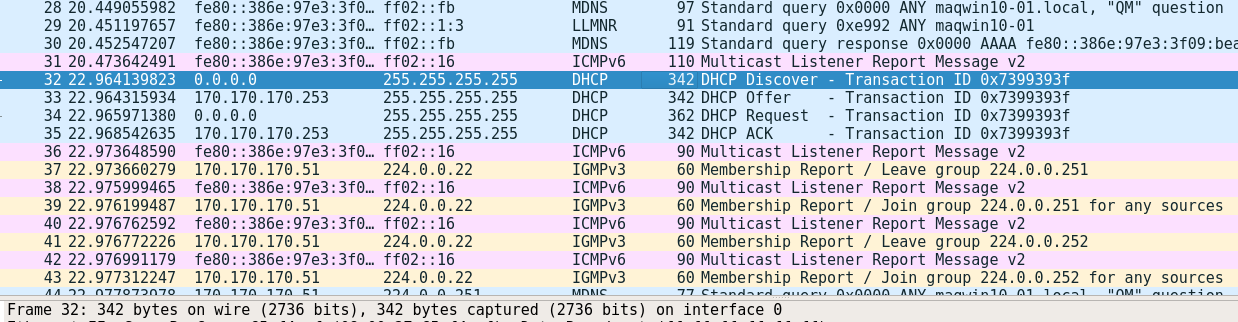


Ahora vamos a instalar wireshark, lo primero cambiamos a nat porque estamos en red interna, lo instalamos.

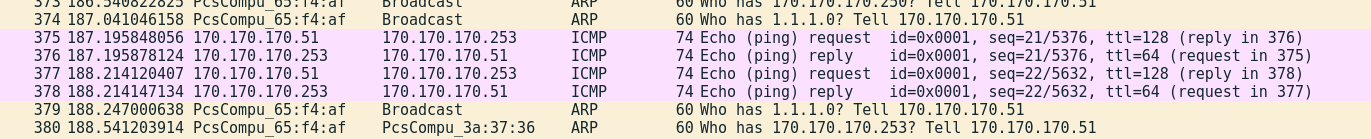
IMPORTANTE, para abrirlo, o lo abrimos como sudo, o tenemos que darle permiso al os usuarios, porque no tenemos permiso, para ello sudo chmod +x *usr/*bin/dumpcat y listo

Ya podemos capturar tramas.

Si en el cliente me quito la ip y le pido una nueva, podemos ver todo el proceso de tramas.

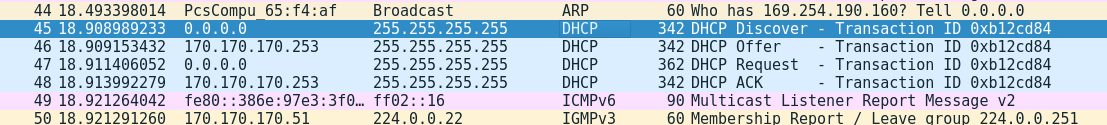


Si pruebo a hacer un ping vemos un icmp



Vamos a ejecutar wireshark para ver las tramas

En el equipo CLIENTE, ahora mismo no tengo IP, asi que solicito una ip con /renew. El wireshark está analizando toda la red y capta esto

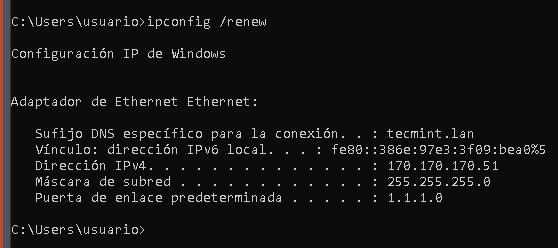


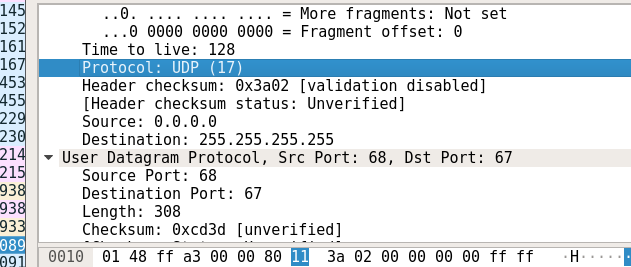
Como vimos ayer, hay alguien sin ip (0,0,0,0) mandando un DHCP discover

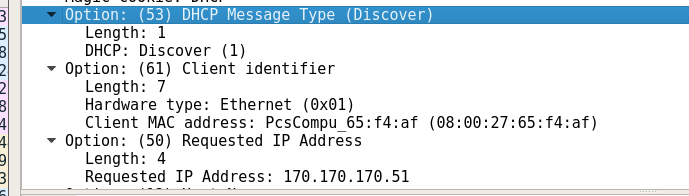
Entonces el servidor DHCP le responde con un Offer y los parámetros correspondientes.

Como solo tenemos 1 DHCP, el cliente le manda un request indicando que acepta la IP

El servidor DHCP le dice que ok.

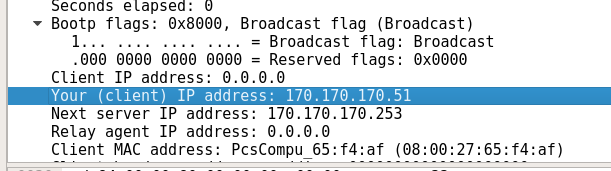


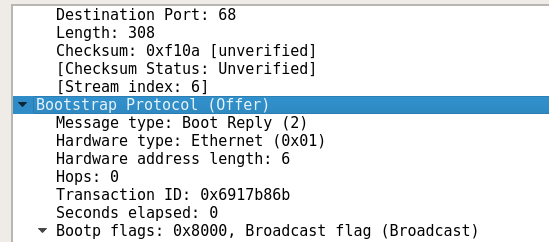
Podemos ir mirando 1 a 1 las 4 tramas para ver su contenido.

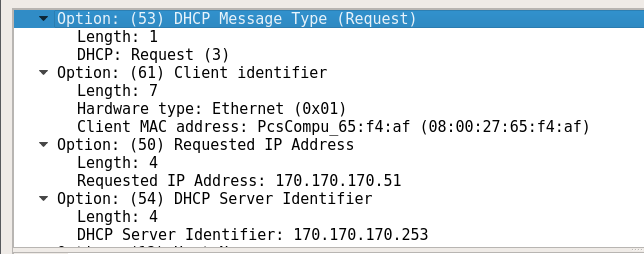


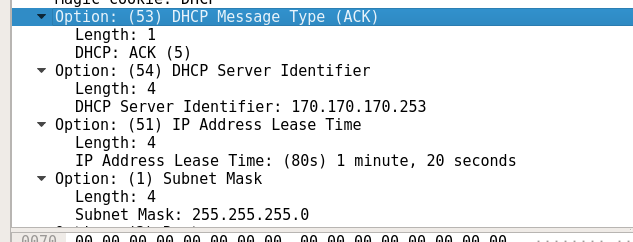
En la trama discover podemos ver un poco todo el contenido: Protocolo empleado, IP origen, IP destino (broadcast), puertos, el TTL, etc.

Si miramos la trama DHCP OFFER, podemos ver como el servidor ve que el cliente no tiene IP, y le manda una IP para él solito, con todas sus demás opciones.



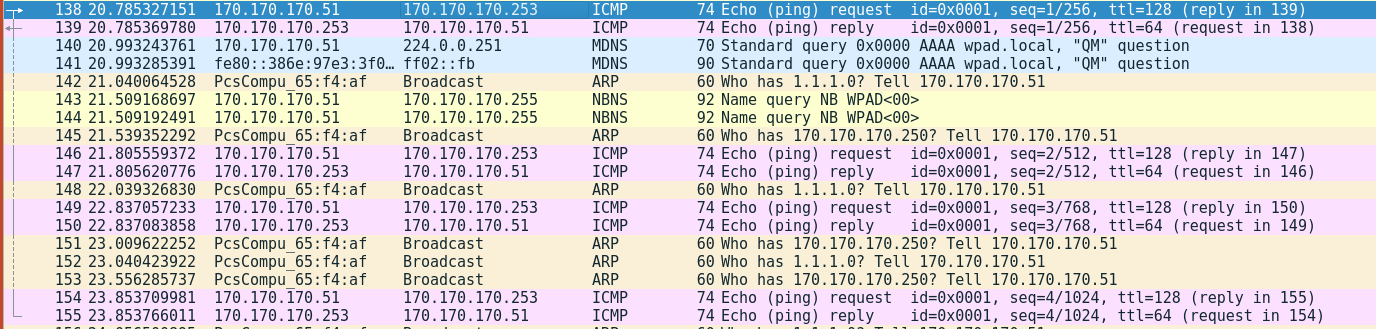




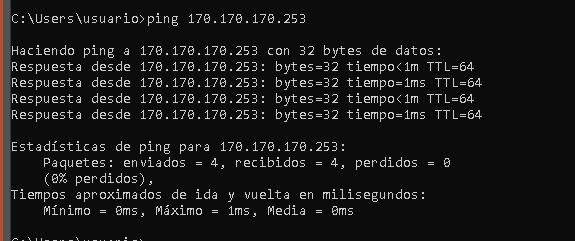
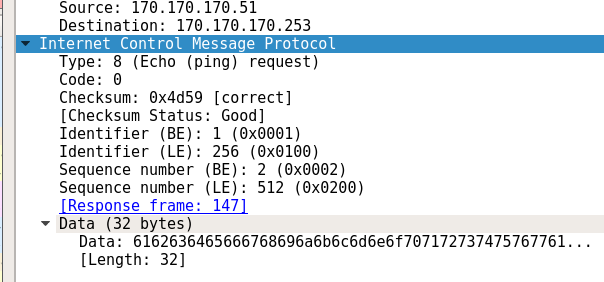


Podemos probar a mandar un PING desde el cliente hasta el servidor DNS

Se mandan el correspondiente ICMP reply y un REQUEST, y comienza el envio del PING



Si lo comparamos al cliente, aquí solo podemos ver el TTL y los bytes, mientras que en wireshark podemos ver TODOS los protocolos que se involucran, y los contenidos de las tramas.

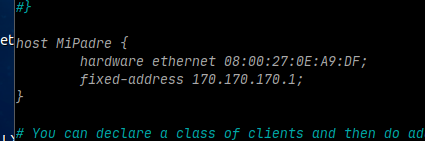


Dato curioso: En la CMD de windows sale TTL 64 todo el rato, mientras que en wireshark salen 128 y 64. Si nos fijamos con detalle, las que aparecen con TTL=64 en wireshark son las tramas REPLY, es decir, las que manda el servidor, y las que vemos en la CMD son las tramas que ha recibido del servidor, osease, es correcto.

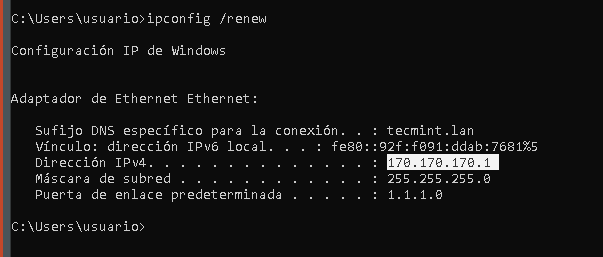
El ping manda 32 bytes según la cmd, y si abrimos la trama, podemos ver la DATA del ping, y efectivamente, hay 32 bits de datos.

A veces puede darse el caso, de que el servidor DHCP mande una trama DHCP NACK → significa no ack, es decir, NO te dejo usar la ip que te he dado.

Podemos asignar Ips estáticas en un servidor DHCP, para ello tenemos que configurar en el archivo de config otras líneas.

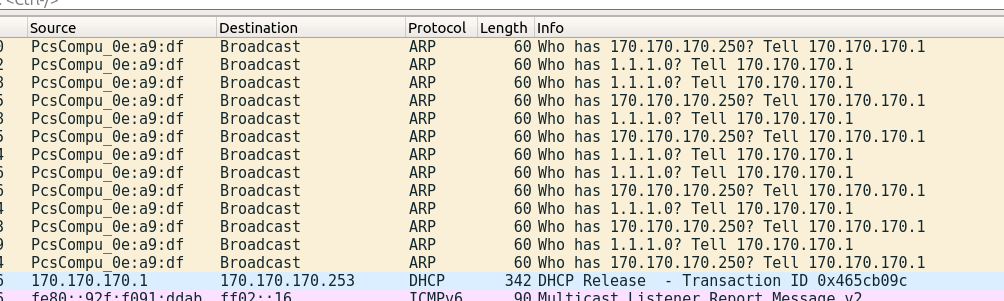


Importante que pongas los 2 puntos, porque los guiones de windows no funcionan.



Estoy dentro de la misma red, y tengo la IP estática asignada.

Con el protocolo ARP se busca, por un lado, conocer las Ips de todos los otros equipos de la red, y otro uso es preguntar quien tiene una IP X y así sabes si la tiene alguien, o si está libre, y por tanto puedes solicitarla



Cuando hacemos un /release seguido de un /renew, se ejecutan los 4 protocolos DHCP que hemos visto, y adicionalmente, posterior a esto, se ejecuta un ARP Gratuitous



Se hace después del DHCP para comprobar que la Ip que te han asignado esta libre, si aparece alguien que ya la tenía, entonces es que tu estas duplicando, y por tanto la soltarás y pedirás una nueva.

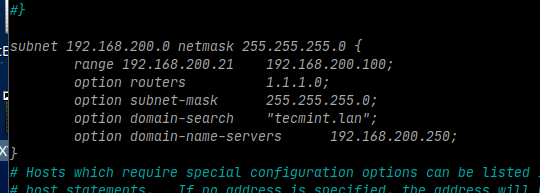
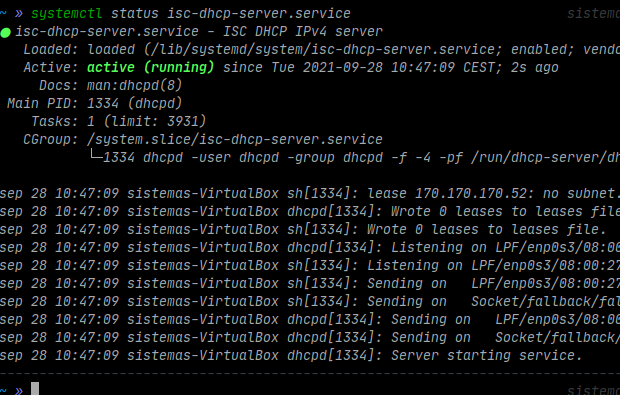
Escenario 1 para hoy

Tener 1 servidor DHCP + 2 clientes corriendo a la vez, para que se hagan peticiones y no tenga 1 cliente solo 1 servidor dhcp para él solito, que comparta. (W10+linux)

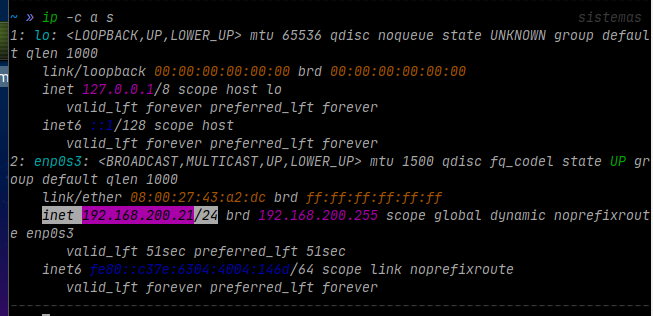
Escenario 2:

Tener 2 servidores DHCP y un cliente, para que el cliente haga lo de elegir un servidor.

Cuando inicies el segundo servidor DHCP, acuérdate de cambiar las ips y el rango en el archivo de confi, que es un clon, ergo es idéntico al primero.



Servidor iniciado y operativo, con esa configuración, arranco los clientes.



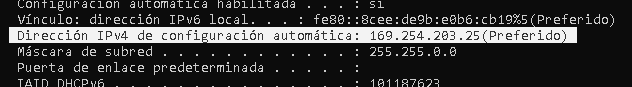
En el cliente linux tengo ya conexión, me ha dado una ip.

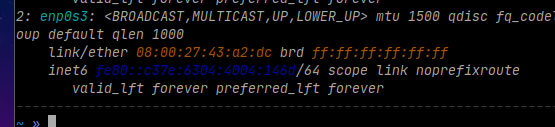


En el cliente windows también tengo conexión, me ha dado una ip.

Vamos a verlo todo ahora en wireshark

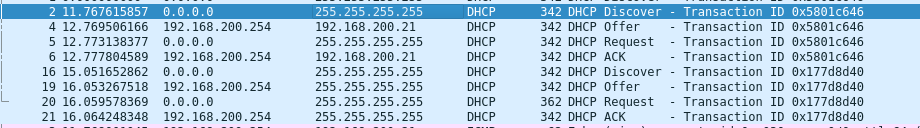
1º → Hacemos ipconfig /release y sudo dhclient -v para quedarnos sin ips en ambos clientes.



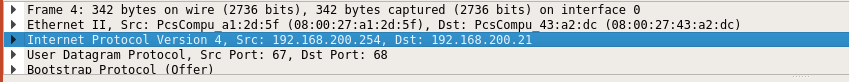
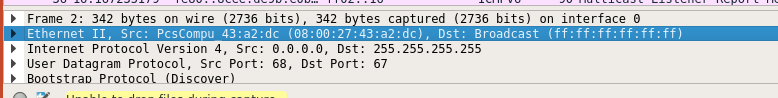


2º → Abrimos wireshark, capturamos trama y conectamos los clientes. Aparece 2 veces el proceso de DHCP protocol.

Si nos fijamos en el contenido de la trama vemos que cada uno es para un cliente.



El primer DHCP es para el cliente linux, le otorga la dirección correspondiente.

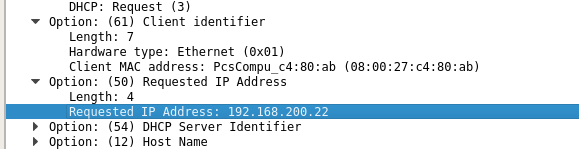
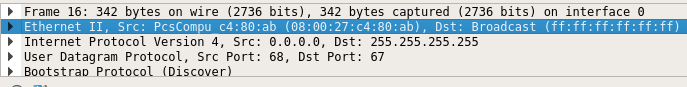


Le ofrece la .21, acepta la trama y se hace el ACK.

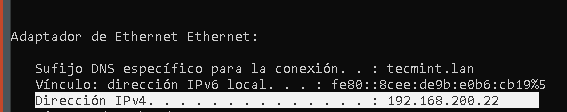


Comprobamos que efectivamente la tiene.

Vamos al siguiente

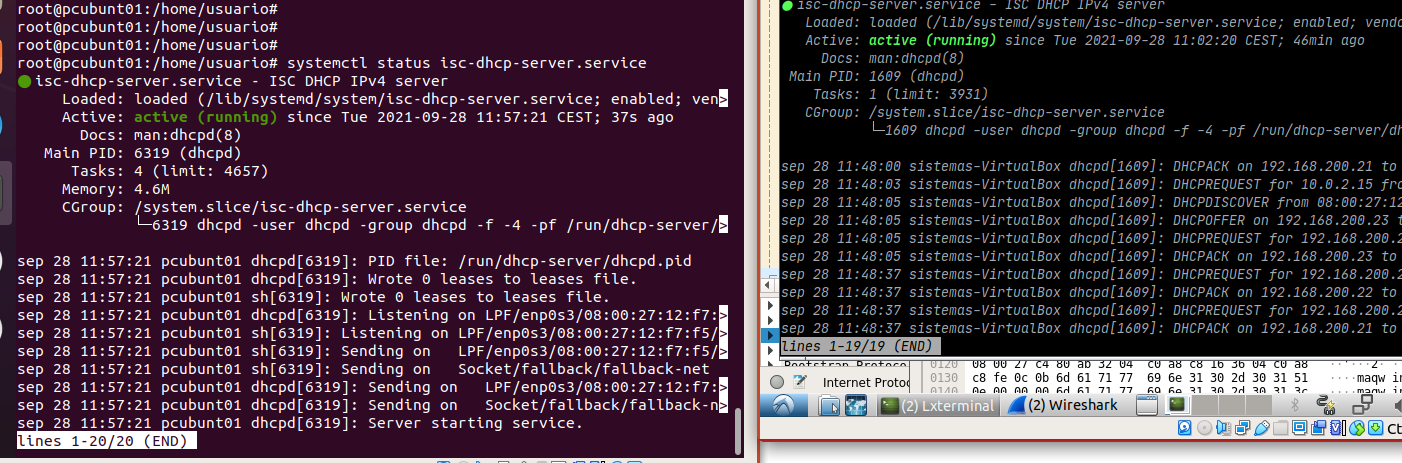


Aquí tenemos la IP del cliente2.

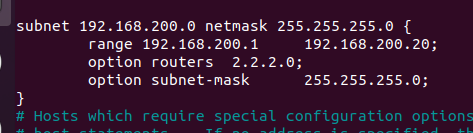


Pasamos al ejercicio 2.

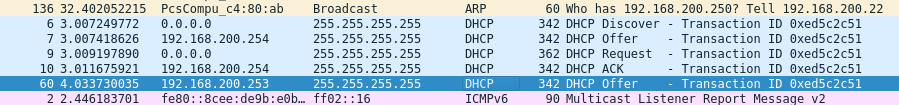
1º → Configuro un nuevo servidor DHCP dentro de la misma red



El primer DHCP es el de antes, tiene la misma configuración. Este nuevo DHCP le he asignado otro rango de direcciones.



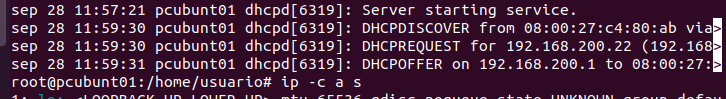
2º → Le quitamos al cliente windows la IP para hacer todo el proceso, y solicitamos una IP a la red.



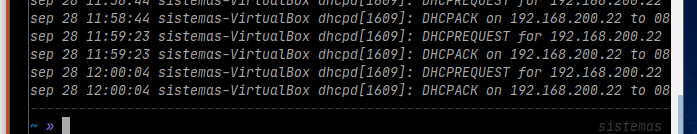
Aquí podemos apreciar que hay 2 DHCP offer, el primero es del servidor 254, que es quien realiza todo el proceso, y luego más tarde llega el servidor 253.

Según tengo entendido, por defecto, está configurado para que los clientes cojan la primera IP que les llegue. Y para evitar que los servidores descartados bombardeen con el DHCP offer a la red, el Request del cliente informa a todos los servidores que ha escogido una red, para que no manden ese broadcast innecesario.

De hecho, me acabo de percatar, en el SYSTEMCTL status, podemos ver los paquetes DHCP, interesante porque podemos ver las peticiones sin necesidad de wireshark, pero no podemos ver el contenido de la trama, asi que es útil pero no mucho.

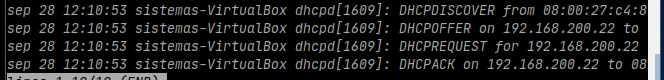


Aquí se puede apreciar como el servidor Ubuntu recibe un discover, y acto seguido recibe un Request del mismo cliente diciendo que ya tiene una IP, justo antes de que el propio servidor le mandase su offer, es decir, se corresponde con lo que vemos en wireshark en la imagen anterior.



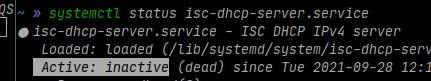
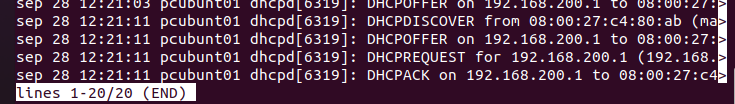
Mientras tanto, el otro servidor está renovando la IP del cliente.

Si vuelvo a liberar la IP, puedo ver aquí también lso paquetes, nuevamente siendo el servidor 1 el más rápido.

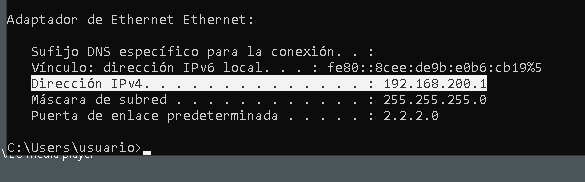


Ahora, dado que ya me funciona todo con los 2 servidores, voy a complicarme yo solito la vida y ver qué pasa, voy a probar a desactivar este DHCP, para que el cliente coja una IP del otro servidor.

El servidor 2 recibe el offer y hace todo el proceso, exactamente igual que antes.



El otro server esta apagado.

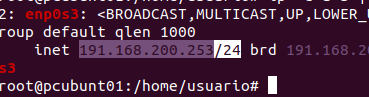


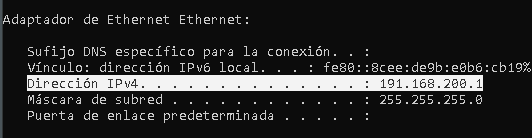
El cliente recibe una IP del otro servidor, genial, funciona.

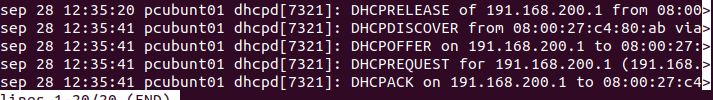
Adicionalmente, voy a probar otra cosa, voy a poner CADA SERVIDOR en una RED DIFERENTE.

El original se queda en la 192, y el segundo, lo pongo en la 191.

1º → Voy a probar que funcione solo 1 servidor, para ver que no hay problemas raros con las ips y las redes.

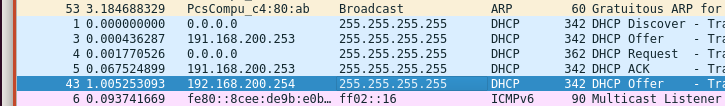






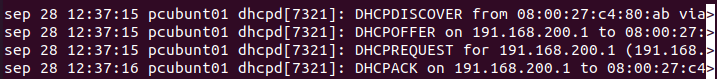
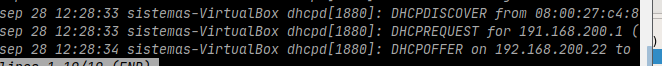
El cliente recibe una IP correctamente de otro rango de red.

Ahora voy a levantar los 2 servidores y voy a ver como se pegan entre ellos por darle una ip al cliente.



Si miramos en wireshark, nuevamente hay 2 offers diferentes, el de la 191 y el de la 192.

El cliente vuelve a coger el de la 191, manda el request y lo recibe el servidor 192.



Al igual que antes, los 2 servidores reciben el DHCP discover, mandan su offer, y uno de los dos se quedará sin poder otorgar direccionamiento al cliente. Con la particularidad de que ahora el ejercicio utiliza DHCPs de diferentes redes.