

1. Análisis del proceso de eliminación automática de parámetros de red

Sabemos que, si tenemos a nuestro Kali por defecto en adaptador puente, éste conectará a nuestro módem, por lo que tendrá una dirección IP mediante DHCP a penas encienda, en este laboratorio usé como router el c3745 de GNS3, y le configuré el DHCP para tener una experiencia como si estuviese trabajando en el router de mi hogar, así lo tengo listo para próximos laboratorios como el ataque dhcp por virginia.

```

root@kali: /home/kali
Archivo Acciones Editar Vista Ayuda
PowerShell 7.1.3
Copyright (c) Microsoft Corporation.

https://aka.ms/powershell
Type 'help' to get help.

(kali@kali)-[/home/kali]
PS> ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:82:de:fc brd ff:ff:ff:ff:ff:ff
    inet 192.168.100.94/24 brd 192.168.100.255 scope global dynamic noprefixroute eth0
        valid_lft 86366sec preferred_lft 86366sec
    inet6 fe80::a00:27ff:fe82:de:fc/64 scope link noprefixroute
        valid_lft forever preferred_lft forever

(kali@kali)-[/home/kali]
PS> ip -a
Usage: ip [ OPTIONS ] OBJECT { COMMAND | help }
       ip [ -force ] -batch filename
where  OBJECT := { address | addrlabel | amt | fou | help | ila | ioam | l2tp |
                  link | macsec | maddress | monitor | mptcp | mroute | mrule |
                  neighbor | neighbour | netconf | netns | nexthop | ntable |
                  ntbl | route | rule | sr | tap | tcpmetrics |
                  token | tunnel | tuntap | vrf | xfrm }
       OPTIONS := { -V[ersion] | -s[tatistics] | -d[etails] | -r[esolve] |
                   -h[uman-readable] | -iec | -j[son] | -p[retty] |
                   -f[amily] { inet | inet6 | mpls | bridge | link } |
                   -4 | -6 | -M | -B | -O |
                   -l[oops] { maximum-addr-flush-attempts } | -br[ief] |
                   -o[neline] | -t[imestamp] | -ts[hort] | -b[atch] [filename] |
                   -rc[vbuf] [size] | -n[etns] name | -N[umeric] | -a[ll] |

```

Fig1. Dirección IP al inicio, respecto a mi modem en casa.

```
R4
R4(config-if)#no shutdown
R4(config-if)#exit
R4(config)#ip dhcp
R4(config)#ip dhcp exc
R4(config)#ip dhcp excluded-address 10.0.0.1
R4(config)#ip dhcp
R4(config)#ip dhcp po
R4(config)#ip dhcp pool DHCP_UNI
R4(dhcp-config)#def
R4(dhcp-config)#default-router 10.0.0.1
R4(dhcp-config)#dns
R4(dhcp-config)#dns-server 8.8.8.8
R4(dhcp-config)#exit
R4(config)#exit
R4#wr
Building configuration...
[OK]
R4#
*Mar  1 00:02:08.051: %SYS-5-CONFIG_I: Configured from console by console
R4#show arp
Protocol Address          Age (min)  Hardware Addr  Type   Interface
Internet 10.0.0.2              1  0050.7966.6801  ARPA   FastEthernet0/0
Internet 10.0.0.1              -  c404.3cec.0000  ARPA   FastEthernet0/0
R4#
```

Fig1. Dirección router de gns3 para que sea el Gateway

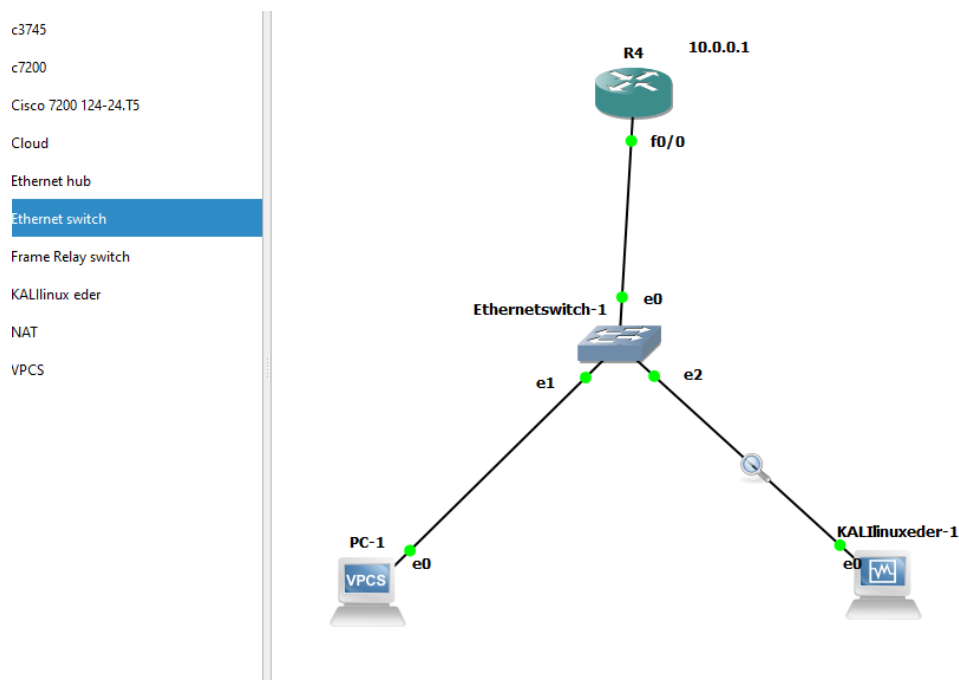
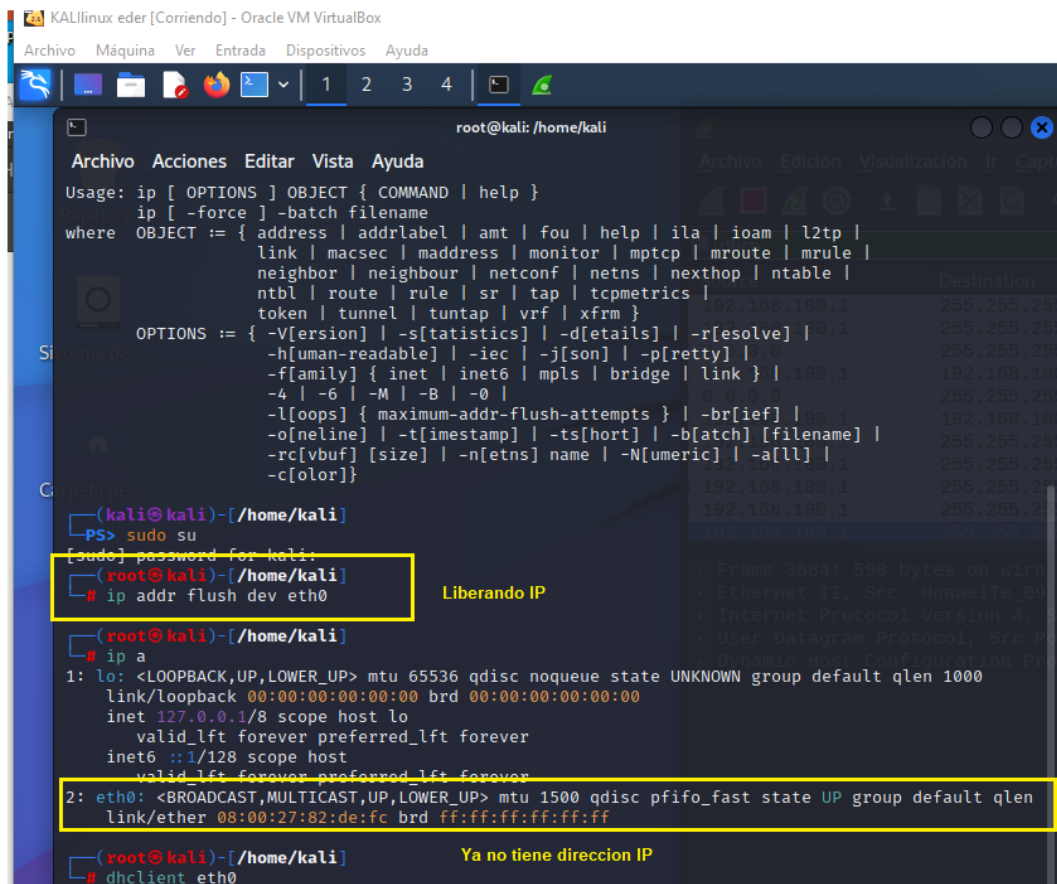


Fig3. Topología de nuestro Laboratorio en GNS3

2. Libere su dirección IP desde la máquina virtual Kali Linux.



```
root@kali: /home/kali
Usage: ip [ OPTIONS ] OBJECT { COMMAND | help }
ip [ -force ] -batch filename
where OBJECT := {
  address | addrlabel | amt | fou | help | ila | ioam | l2tp |
  link | macsec | maddress | monitor | mptcp | mroute | mrule |
  neighbor | neighbour | netconf | netns | nexthop | ntable |
  ntbl | route | rule | sr | tap | tcpmetrics |
  token | tunnel | tuntap | vrf | xfrm }
OPTIONS := {
  -V[ersion] | -s[tatistics] | -d[etails] | -r[esolve] |
  -h[uman-readable] | -iec | -j[son] | -p[retty] |
  -f[amily] { inet | inet6 | mpls | bridge | link } |
  -4 | -6 | -M | -B | -0 |
  -l[oops] { maximum-addr-flush-attempts } | -b[rief] |
  -o[neline] | -t[imestamp] | -ts[hort] | -b[atch] [filename] |
  -rc[vbuf] [size] | -n[etns] name | -N[umeric] | -a[ll] |
  -c[olor]}

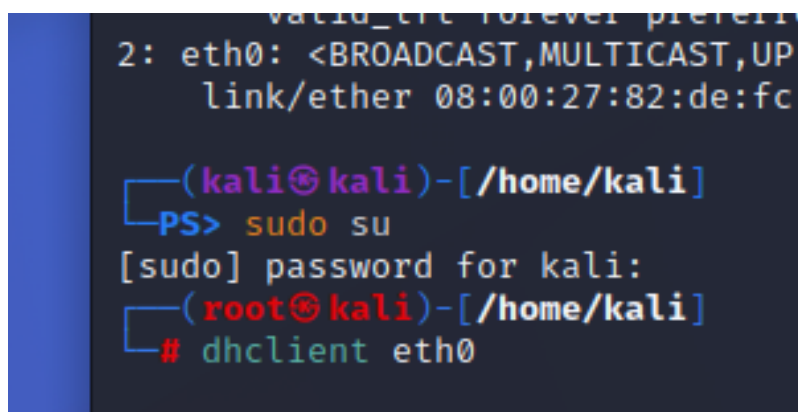
(kali@kali)-[/home/kali]
PS> sudo su
[sudo] password for kali:
(root@kali)-[/home/kali]
# ip addr flush dev eth0
Liberando IP

(root@kali)-[/home/kali]
# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
   link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
   inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
   inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen
   link/ether 08:00:27:82:de:fc brd ff:ff:ff:ff:ff:ff
Ya no tiene direccion IP

(root@kali)-[/home/kali]
# dhclient eth0
```

Fig4. Libero la IP de mi Kali y configuro para que tenga conexión con mi router de GNS3

3. Inicie el proceso de solicitud para la reparación de parámetros de red mediante DHCP.



```
valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen
   link/ether 08:00:27:82:de:fc brd ff:ff:ff:ff:ff:ff

(kali@kali)-[/home/kali]
PS> sudo su
[sudo] password for kali:
(root@kali)-[/home/kali]
# dhclient eth0
```

Fig5. Uso el comando dhclient seguido de la interfaz para obtener una dirección IP mediante protocolo dhcp

4. Capture el tráfico de red en la máquina virtual Kali linux mediante la herramienta Wireshark

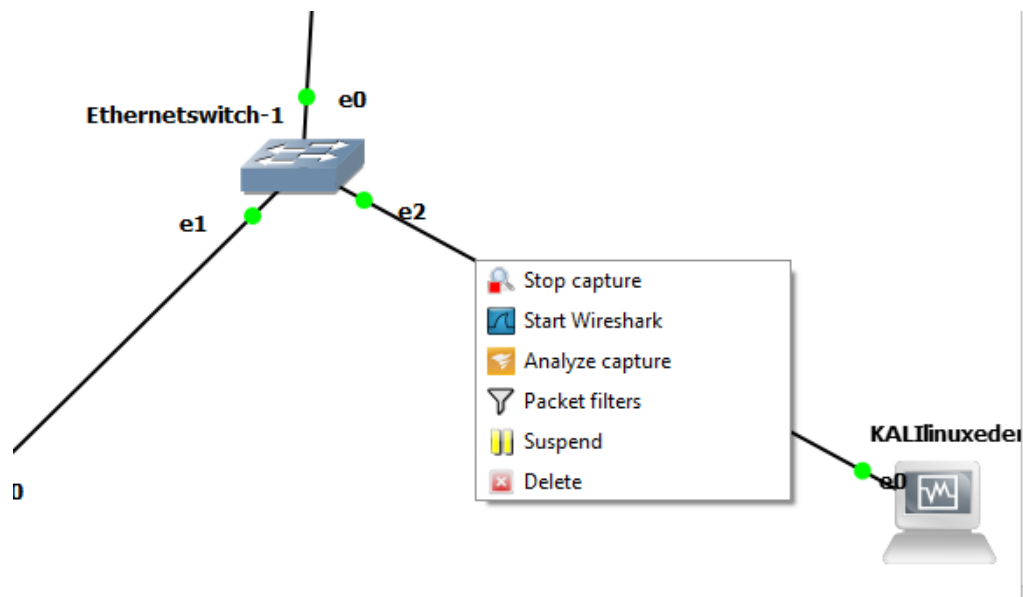


Fig6. Uso Wireshark en mi enlace

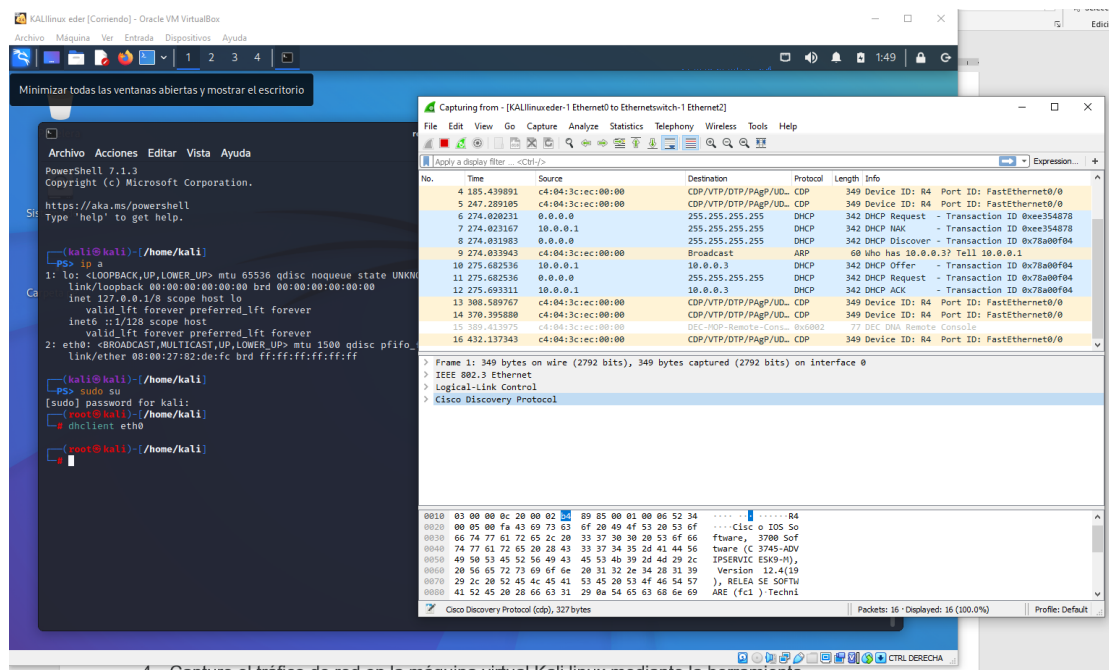


Fig7. Análisis del Wireshark

Capturing from - [KaliLinuxer-1 Ethernet0 to Ethernetswitch-1 Ethernet2]

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/> Expression...

No.	Time	Source	Destination	Protocol	Length	Info
8	274.031983	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x78a00f04
9	274.033943	c4:04:3c:ec:00:00	Broadcast	ARP	60	Who has 10.0.0.3? Tell 10.0.0.1
10	275.682536	10.0.0.1	10.0.0.3	DHCP	342	DHCP Offer - Transaction ID 0x78a00f04
11	275.682536	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0x78a00f04
12	275.693311	10.0.0.1	10.0.0.3	DHCP	342	DHCP ACK - Transaction ID 0x78a00f04
13	308.589767	c4:04:3c:ec:00:00	CDP/VTP/DTP/PagP/UD...	CDP	349	Device ID: R4 Port ID: FastEthernet0/0
14	370.395880	c4:04:3c:ec:00:00	CDP/VTP/DTP/PagP/UD...	CDP	349	Device ID: R4 Port ID: FastEthernet0/0
15	389.413975	c4:04:3c:ec:00:00	DEC-NOP-Remote-Cons...	0x6002	77	DEC DNA Remote Console
16	432.137343	c4:04:3c:ec:00:00	CDP/VTP/DTP/PagP/UD...	CDP	349	Device ID: R4 Port ID: FastEthernet0/0
17	493.982638	c4:04:3c:ec:00:00	CDP/VTP/DTP/PagP/UD...	CDP	349	Device ID: R4 Port ID: FastEthernet0/0
18	555.982704	c4:04:3c:ec:00:00	CDP/VTP/DTP/PagP/UD...	CDP	349	Device ID: R4 Port ID: FastEthernet0/0
19	617.831918	c4:04:3c:ec:00:00	CDP/VTP/DTP/PagP/UD...	CDP	349	Device ID: R4 Port ID: FastEthernet0/0
20	679.622359	c4:04:3c:ec:00:00	CDP/VTP/DTP/PagP/UD...	CDP	349	Device ID: R4 Port ID: FastEthernet0/0

> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 Total Length: 328
 Identification: 0x0005 (5)
 > Flags: 0x0000
 Time to live: 255
 Protocol: UDP (17)
 Header checksum: 0xa69c [validation disabled]
 [Header checksum status: Unverified]
 Source: 10.0.0.1
 Destination: 10.0.0.3
 > User Datagram Protocol, Src Port: 67, Dst Port: 68
 > Dynamic Host Configuration Protocol (ACK)

Fig8. Aparición de DORA, en el Wireshark.

```

R4
R4(config)#ip dhcp
R4(config)#ip dhcp po
R4(config)#ip dhcp pool DHCP_UNI
R4(dhcp-config)#def
R4(dhcp-config)#default-router 10.0.0.1
R4(dhcp-config)#dns
R4(dhcp-config)#dns-server 8.8.8.8
R4(dhcp-config)#exit
R4(config)#exit
R4#wr
Building configuration...
[OK]
R4#
*Mar 1 00:02:08.051: %SYS-5-CONFIG_I: Configured from console by console
R4#show arp
Protocol Address Age (min) Hardware Addr Type Interface
Internet 10.0.0.2 1 0050.7966.6801 ARPA FastEthernet0/0
Internet 10.0.0.1 - c404.3cec.0000 ARPA FastEthernet0/0
R4#show arp
Protocol Address Age (min) Hardware Addr Type Interface
Internet 10.0.0.2 18 0050.7966.6801 ARPA FastEthernet0/0
Internet 10.0.0.3 11 0800.2782.defc ARPA FastEthernet0/0
Internet 10.0.0.1 - c404.3cec.0000 ARPA FastEthernet0/0
R4#

```

Fig9. Tabla ARP, después de la asignación de IP mediante dhcp a mi kali