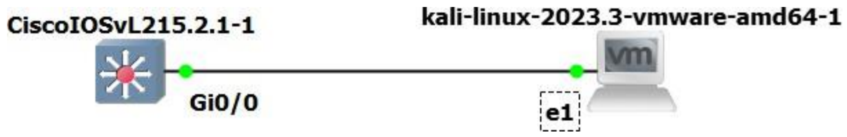
TP4 : Hacking réseau et les contre-mesures

TP 4.1: MAC flooding

Architecture réseau

- Un L2 Switch
- VM Kali (PC Hacker)
- Une connexion à internet (optionnel).



Les étapes du TP :

- Ouvrir l'émulateur GNS3
- Sélectionner L2 switcheur
- Sélectionner la machine kali linux (pc hacker) qui est déjà importée à l'émulateur.
- Lier les deux équipements avec un câble Ethernet.
- Démarrer tous les équipements.

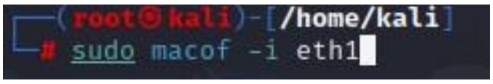
Vérification de l'état du switcher

Switch#show mac address-table

Installation de l'outil macof

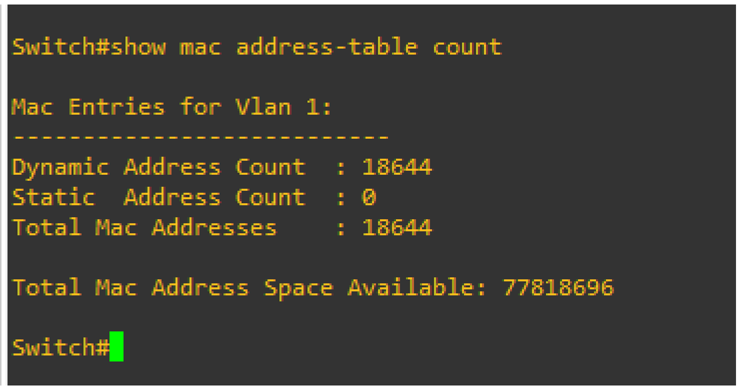
apt-get install dsniff

Lancer l'attaque MAC flooding



```
┌──(root㉿kali)-[/home/kali]
└─# sudo macof -i eth1
```

Switch#show mac address-table



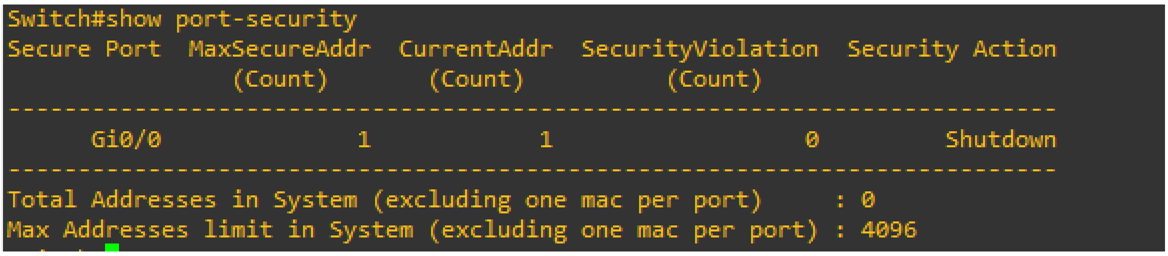
```
Switch#show mac address-table count

Mac Entries for Vlan 1:
---------------------------
Dynamic Address Count  : 18644
Static  Address Count  : 0
Total Mac Addresses    : 18644

Total Mac Address Space Available: 77818696

Switch#
```

Pour vider la table MAC

Switch# clear mac address-table dynamic

Les contre-mesures pour arrêter ce type d'attaque est : port security

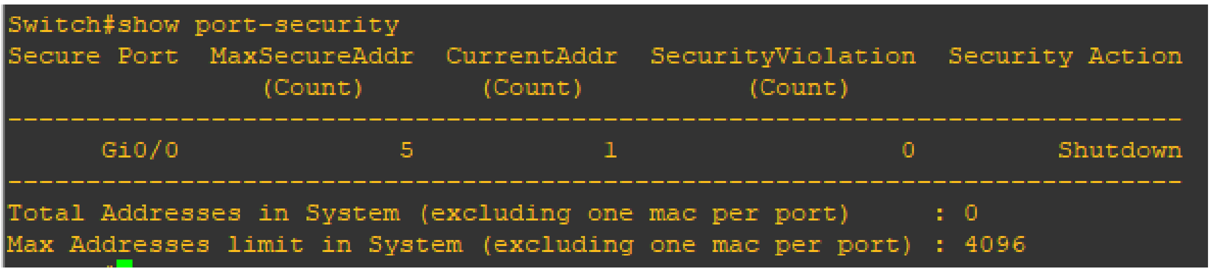
```
Switch>en
Switch# conf t
Switch(config)#interface gigabitEthernet 0/0
Switch(config-if)# switchport mode access
Switch(config-if)# switchport port-security
```



```
Switch#show port-security
Secure Port  MaxSecureAddr  CurrentAddr  SecurityViolation  Security Action
                (Count)       (Count)          (Count)
---------------------------------------------------------------------------
      Gi0/0              1            1                  0         Shutdown
---------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 4096
```

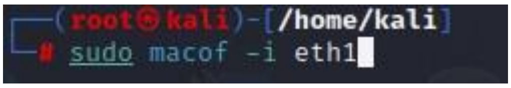
Switch(config-if)#switchport port-security maximum 5

(Le port accepte uniquement 5 adresses MAC)

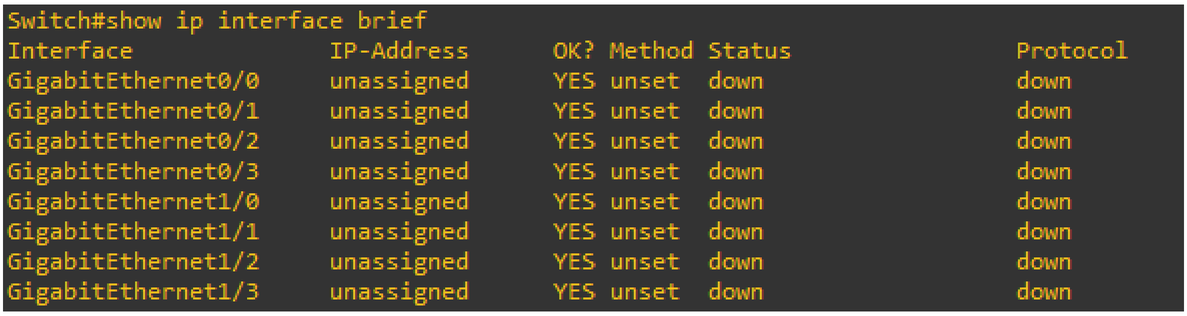


```
Switch#show port-security
Secure Port  MaxSecureAddr  CurrentAddr  SecurityViolation  Security Action
                (Count)        (Count)          (Count)
---------------------------------------------------------------------------
      Gi0/0              5            1                  0         Shutdown
---------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 4096
```

Lancer l'attaque depuis la machine kali



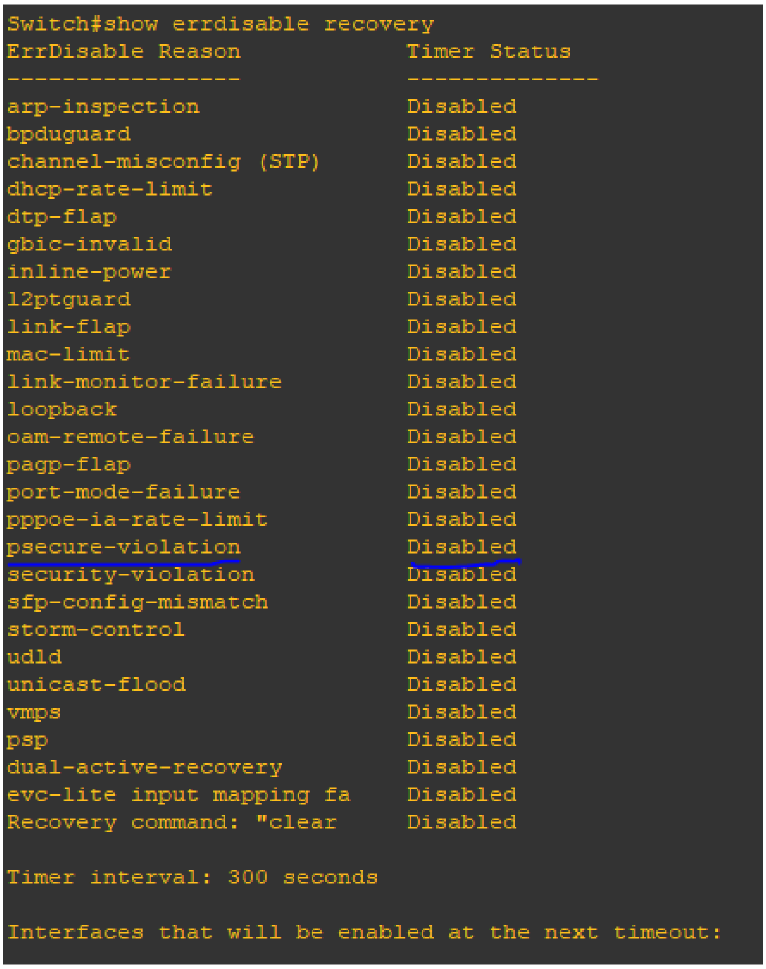
```
┌──(root㉿kali)-[/home/kali]
└─# sudo macof -i eth1
```



```
Switch#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0     unassigned      YES unset  down                  down
GigabitEthernet0/1     unassigned      YES unset  down                  down
GigabitEthernet0/2     unassigned      YES unset  down                  down
GigabitEthernet0/3     unassigned      YES unset  down                  down
GigabitEthernet1/0     unassigned      YES unset  down                  down
GigabitEthernet1/1     unassigned      YES unset  down                  down
GigabitEthernet1/2     unassigned      YES unset  down                  down
GigabitEthernet1/3     unassigned      YES unset  down                  down
```

Le ports g0/0 est actuellement down

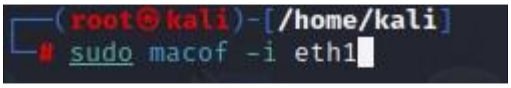
Switch#show errdisable recovery



```
Switch#show errdisable recovery
ErrDisable Reason            Timer Status
-----------------            --------------
arp-inspection               Disabled
bpduguard                    Disabled
channel-misconfig (STP)      Disabled
dhcp-rate-limit              Disabled
dtp-flap                     Disabled
gbic-invalid                 Disabled
inline-power                 Disabled
l2ptguard                    Disabled
link-flap                    Disabled
mac-limit                    Disabled
link-monitor-failure         Disabled
loopback                     Disabled
oam-remote-failure           Disabled
pagp-flap                    Disabled
port-mode-failure            Disabled
pppoe-ia-rate-limit          Disabled
psecure-violation            Disabled
security-violation           Disabled
sfp-config-mismatch          Disabled
storm-control                Disabled
udld                         Disabled
unicast-flood                Disabled
vmps                         Disabled
psp                          Disabled
dual-active-recovery         Disabled
evc-lite input mapping fa    Disabled
Recovery command: "clear     Disabled

Timer interval: 300 seconds

Interfaces that will be enabled at the next timeout:
```

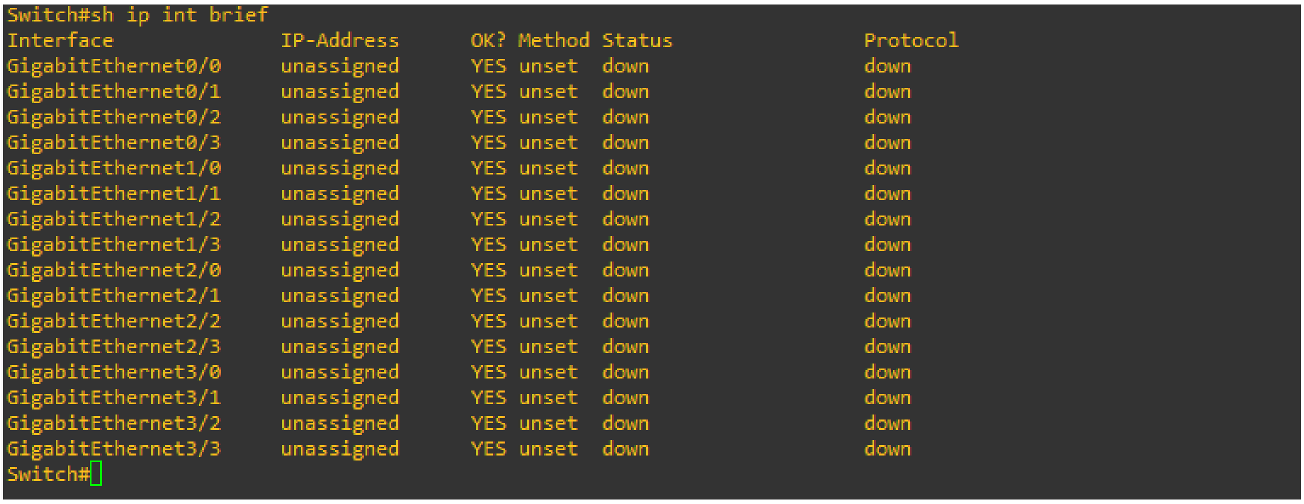
```
Switch(config-if)#switchport port-security aging type inactivity
Switch(config-if)#switchport port-security aging time 5
Switch(config-if)#exit
Switch(config)#errdisable recovery cause psecure-violation
Switch(config)#errdisable recovery interval 60
```

Lancer l'attaque depuis la machine kali



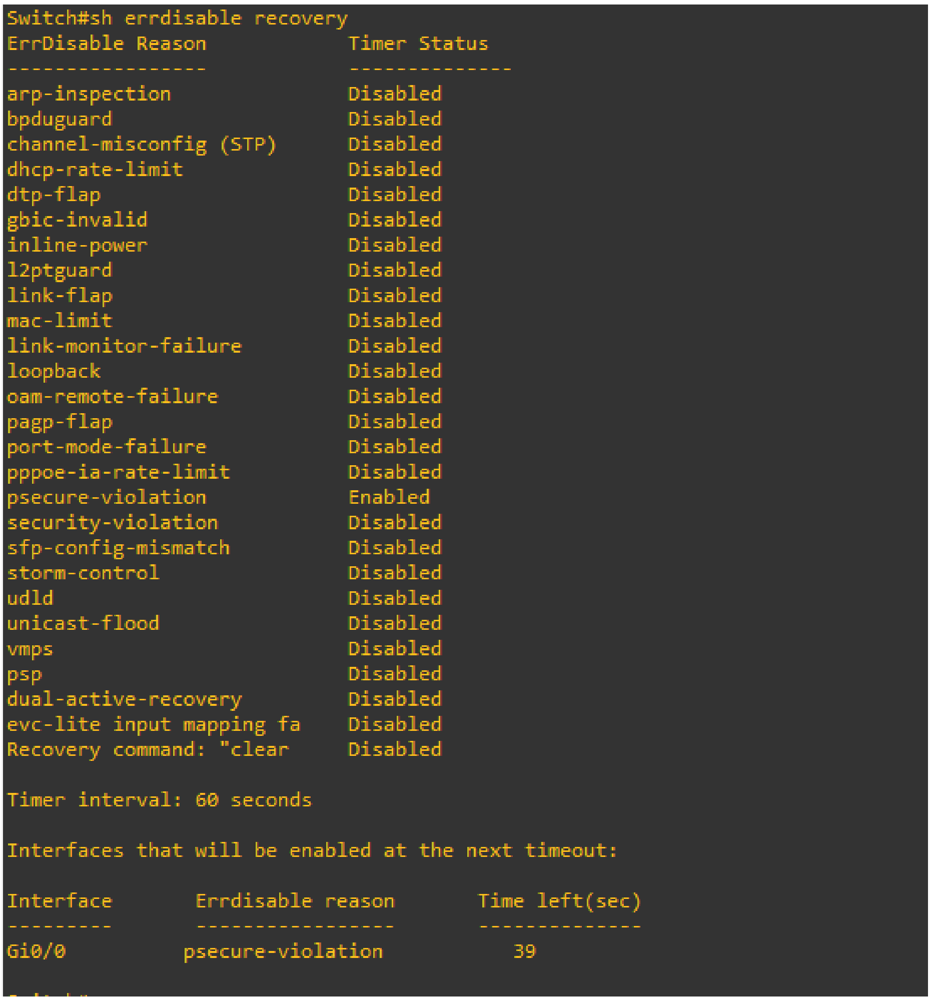
```
┌──(root㉿kali)-[/home/kali]
└─# sudo macof -i eth1
```

Switch#sh ip int brief



```
Switch#sh ip int brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0     unassigned      YES unset  down                  down
GigabitEthernet0/1     unassigned      YES unset  down                  down
GigabitEthernet0/2     unassigned      YES unset  down                  down
GigabitEthernet0/3     unassigned      YES unset  down                  down
GigabitEthernet1/0     unassigned      YES unset  down                  down
GigabitEthernet1/1     unassigned      YES unset  down                  down
GigabitEthernet1/2     unassigned      YES unset  down                  down
GigabitEthernet1/3     unassigned      YES unset  down                  down
GigabitEthernet2/0     unassigned      YES unset  down                  down
GigabitEthernet2/1     unassigned      YES unset  down                  down
GigabitEthernet2/2     unassigned      YES unset  down                  down
GigabitEthernet2/3     unassigned      YES unset  down                  down
GigabitEthernet3/0     unassigned      YES unset  down                  down
GigabitEthernet3/1     unassigned      YES unset  down                  down
GigabitEthernet3/2     unassigned      YES unset  down                  down
GigabitEthernet3/3     unassigned      YES unset  down                  down
Switch#
```

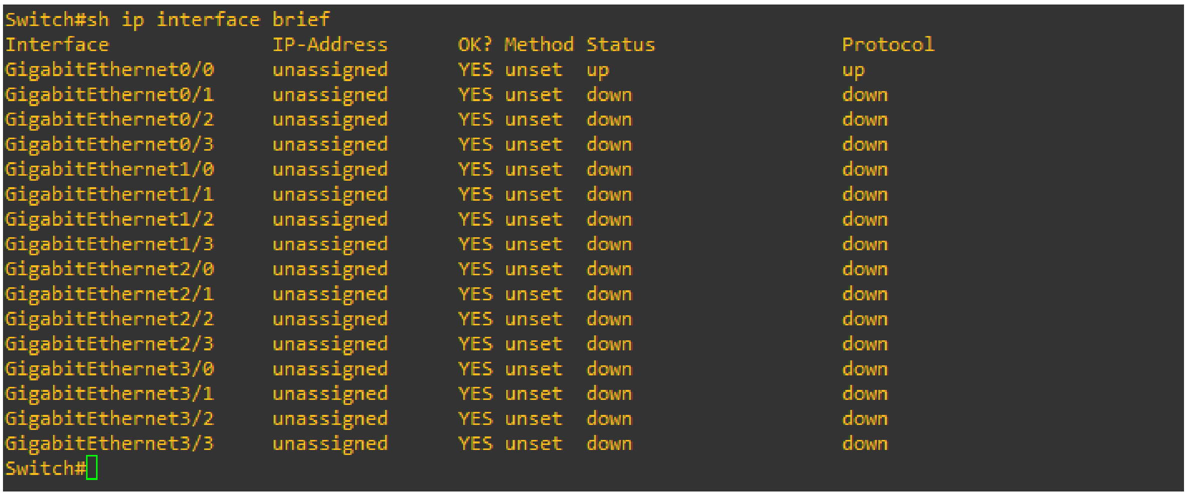
Switch#sh errdisable recovery



```
Switch#sh errdisable recovery
ErrDisable Reason            Timer Status
-----------------            --------------
arp-inspection               Disabled
bpduguard                    Disabled
channel-misconfig (STP)      Disabled
dhcp-rate-limit              Disabled
dtp-flap                     Disabled
gbic-invalid                 Disabled
inline-power                 Disabled
l2ptguard                    Disabled
link-flap                    Disabled
mac-limit                    Disabled
link-monitor-failure         Disabled
loopback                     Disabled
oam-remote-failure           Disabled
pagp-flap                    Disabled
port-mode-failure            Disabled
pppoe-ia-rate-limit          Disabled
psecure-violation            Enabled
security-violation           Disabled
sfp-config-mismatch          Disabled
storm-control                Disabled
udld                         Disabled
unicast-flood                Disabled
vmps                         Disabled
psp                          Disabled
dual-active-recovery         Disabled
evc-lite input mapping fa    Disabled
Recovery command: "clear     Disabled

Timer interval: 60 seconds

Interfaces that will be enabled at the next timeout:

Interface       Errdisable reason       Time left(sec)
---------       -----------------       --------------
Gi0/0          psecure-violation           39
```

Vérification après une minute

Switch# sh ip interface brief

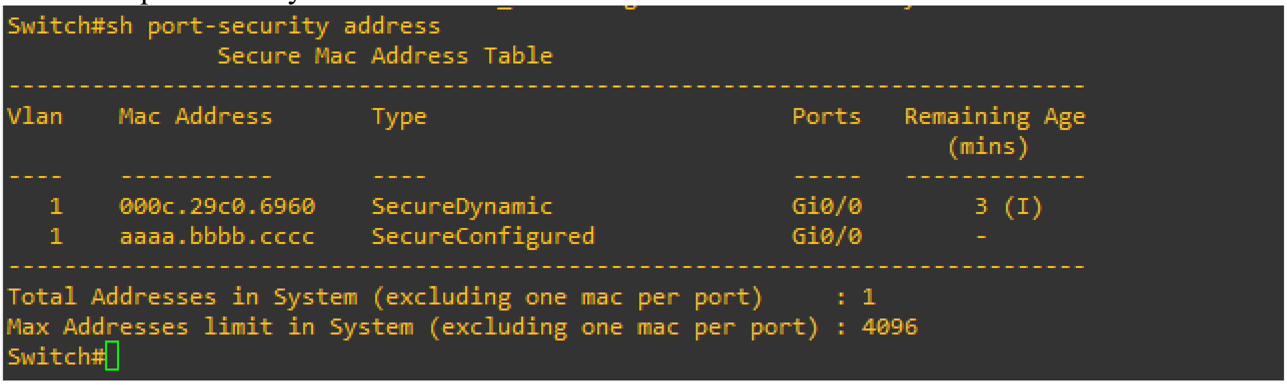


```
Switch#sh ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0     unassigned      YES unset  up                    up
GigabitEthernet0/1     unassigned      YES unset  down                  down
GigabitEthernet0/2     unassigned      YES unset  down                  down
GigabitEthernet0/3     unassigned      YES unset  down                  down
GigabitEthernet1/0     unassigned      YES unset  down                  down
GigabitEthernet1/1     unassigned      YES unset  down                  down
GigabitEthernet1/2     unassigned      YES unset  down                  down
GigabitEthernet1/3     unassigned      YES unset  down                  down
GigabitEthernet2/0     unassigned      YES unset  down                  down
GigabitEthernet2/1     unassigned      YES unset  down                  down
GigabitEthernet2/2     unassigned      YES unset  down                  down
GigabitEthernet2/3     unassigned      YES unset  down                  down
GigabitEthernet3/0     unassigned      YES unset  down                  down
GigabitEthernet3/1     unassigned      YES unset  down                  down
GigabitEthernet3/2     unassigned      YES unset  down                  down
GigabitEthernet3/3     unassigned      YES unset  down                  down
Switch#
```

Ajout des adresses MAC statiquement

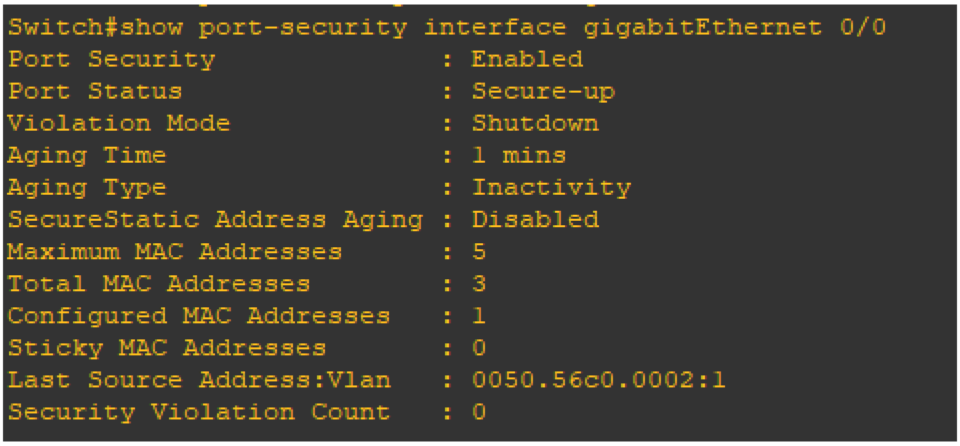
Switch(config-if)#switchport port-security mac-address AAAA.BBBB.CCCC

Switch#sh port-security address



```
Switch#sh port-security address
               Secure Mac Address Table
-----------------------------------------------------------------------------
Vlan    Mac Address       Type                          Ports   Remaining Age
                                                                   (mins)
----    -----------       ----                          -----   -------------
   1    000c.29c0.6960    SecureDynamic                 Gi0/0        3 (I)
   1    aaaa.bbbb.cccc    SecureConfigured              Gi0/0        -
-----------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 1
Max Addresses limit in System (excluding one mac per port) : 4096
Switch#
```

Switch#show port-security interface gi0/0



```
Switch#show port-security interface gigabitEthernet 0/0
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Shutdown
Aging Time                 : 1 mins
Aging Type                 : Inactivity
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 5
Total MAC Addresses        : 3
Configured MAC Addresses   : 1
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 0050.56c0.0002:1
Security Violation Count   : 0
```

Activation d’apprentissage dynamique des adresses MAC.

Switch(config-if)#switchport port-security mac-address sticky

Activation de port security a un port trunk

```
Switch(config-if)#switchport trunk encapsulation dot1q
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport port-security maximum 50
Switch(config-if)#switchport port-security
```

Changement de comportement par défaut de port security

```
Switch#conf t

Switch(config)#interface gigabitEthernet 0/0
Switch(config-if)#switchport port-security violation ?
protect Security violation protect mode
restrict Security violation restrict mode
shutdown Security violation shutdown
```

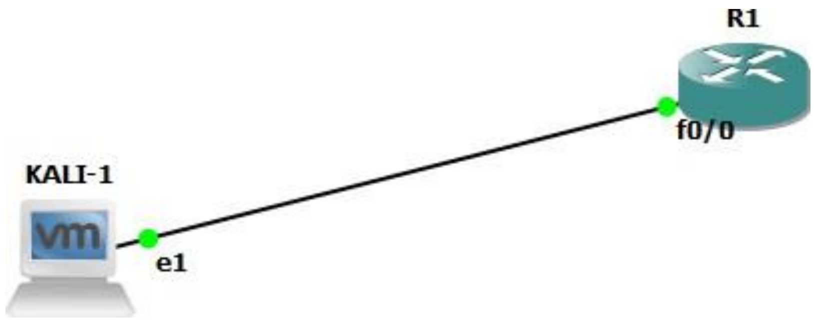
Vérifier la différence entre le mode protect et mode restrict.

TP 4.2 : DHCP starvation

Architecture réseau:

- Un Routeur cisco configurant le DHCP f0 /0
- VM Kali (PC Hacker)

Figure:



Les étapes du TP :

- Ouvrir l'émulateur GNS3
- Sélectionner un routeur (serveur DHCP)
- Sélectionner la machine kali linux (pc hacker) qui est déjà importé à l'émulateur.
- Lier les deux équipements avec un câble Ethernet
- Démarrer tous.

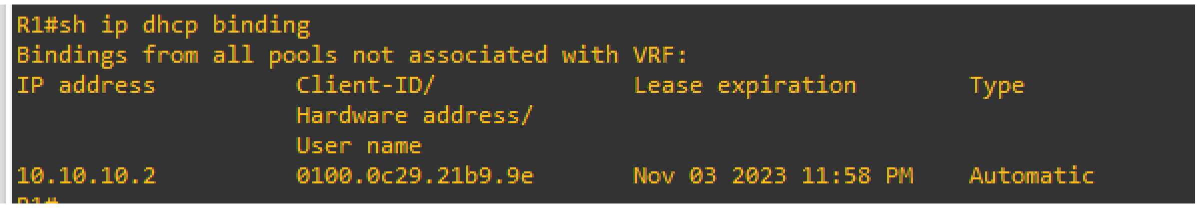
La Configuration du routeur et activation du serveur DHCP

```
Router>en
Router#conf t
Router(config)#interface fastEthernet 0/0
Router(config-if)# ip address 10.10.10.1 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)# ip dhcp pool dhcp-tp
Router(dhcp-config)# network 10.10.10.0 255.255.255.0
Router(dhcp-config)# dns-server 8.8.8.8
Router(dhcp-config)#  default-router 10.10.10.1
```

Router(config-if)#exit

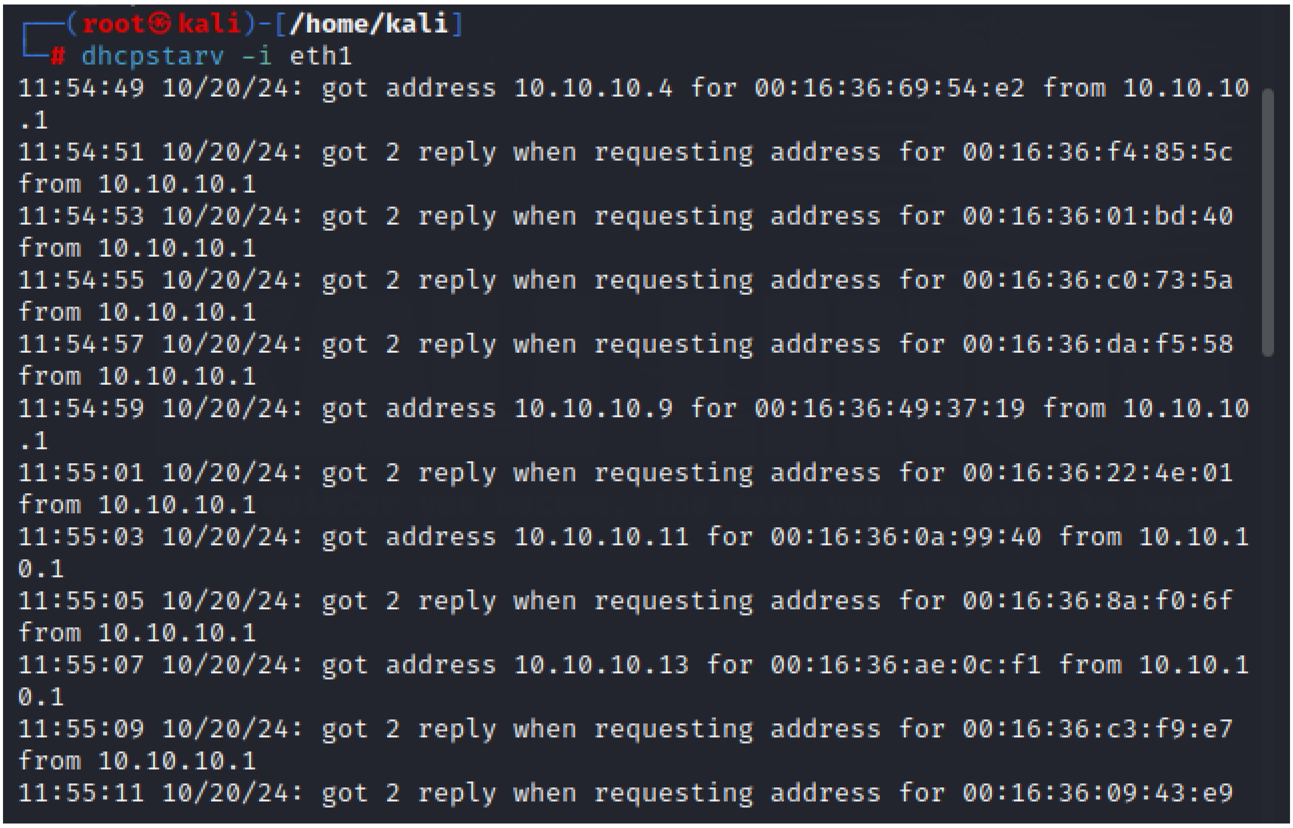
Router(config)#exit

Router#show ip dhcp binding



```
R1#sh ip dhcp binding
Bindings from all pools not associated with VRF:
IP address          Client-ID/              Lease expiration        Type
                    Hardware address/
                    User name
10.10.10.2          0100.0c29.21b9.9e       Nov 03 2023 11:58 PM    Automatic
R1#
```

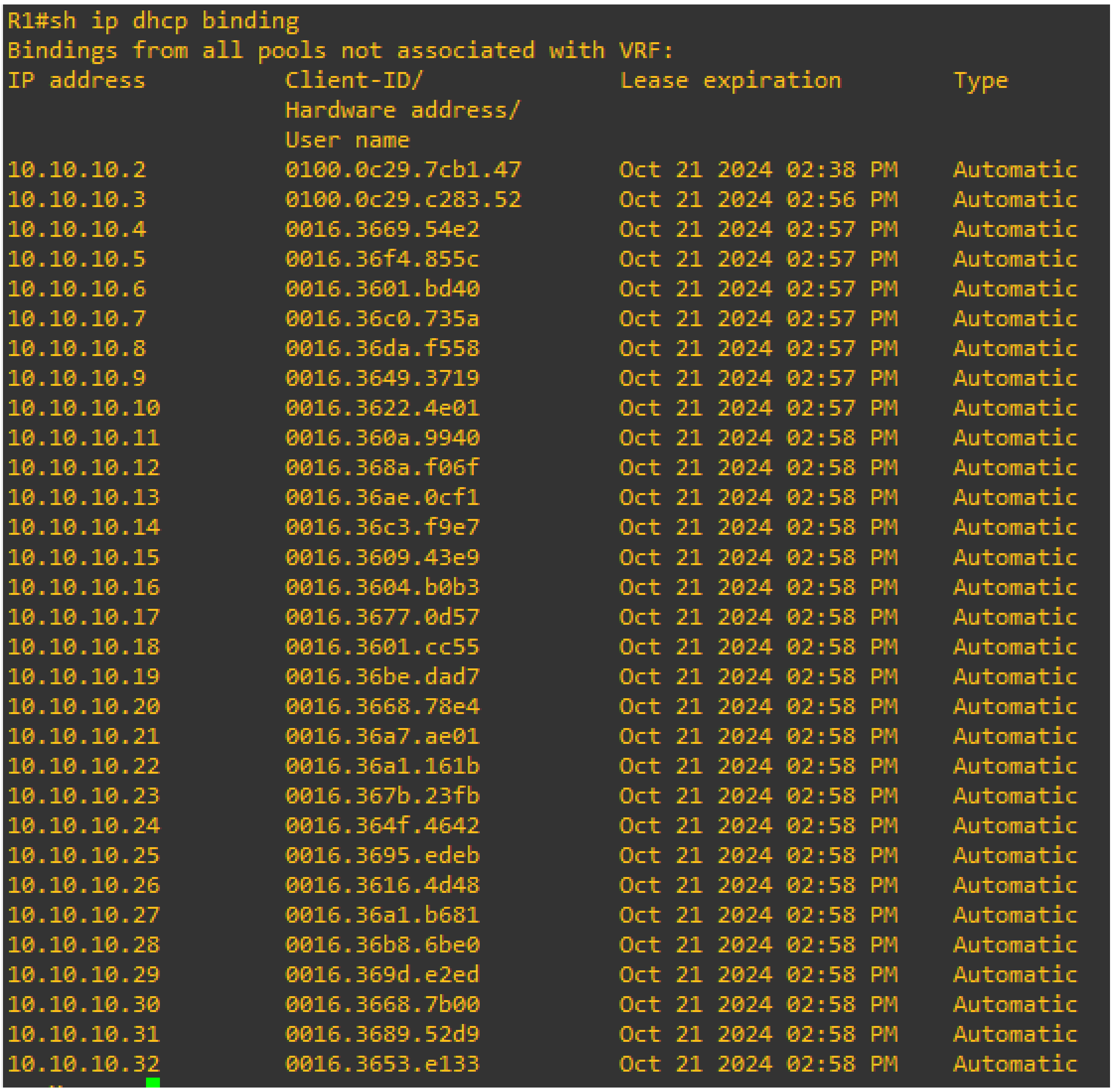
À partir de la machine kali on va lancer l'attaque DHCP STARVATION



```
┌──(root㉿kali)-[/home/kali]
└─# dhcpstarv -i eth1
11:54:49 10/20/24: got address 10.10.10.4 for 00:16:36:69:54:e2 from 10.10.10
.1
11:54:51 10/20/24: got 2 reply when requesting address for 00:16:36:f4:85:5c
from 10.10.10.1
11:54:53 10/20/24: got 2 reply when requesting address for 00:16:36:01:bd:40
from 10.10.10.1
11:54:55 10/20/24: got 2 reply when requesting address for 00:16:36:c0:73:5a
from 10.10.10.1
11:54:57 10/20/24: got 2 reply when requesting address for 00:16:36:da:f5:58
from 10.10.10.1
11:54:59 10/20/24: got address 10.10.10.9 for 00:16:36:49:37:19 from 10.10.10
.1
11:55:01 10/20/24: got 2 reply when requesting address for 00:16:36:22:4e:01
from 10.10.10.1
11:55:03 10/20/24: got address 10.10.10.11 for 00:16:36:0a:99:40 from 10.10.1
0.1
11:55:05 10/20/24: got 2 reply when requesting address for 00:16:36:8a:f0:6f
from 10.10.10.1
11:55:07 10/20/24: got address 10.10.10.13 for 00:16:36:ae:0c:f1 from 10.10.1
0.1
11:55:09 10/20/24: got 2 reply when requesting address for 00:16:36:c3:f9:e7
from 10.10.10.1
11:55:11 10/20/24: got 2 reply when requesting address for 00:16:36:09:43:e9
```

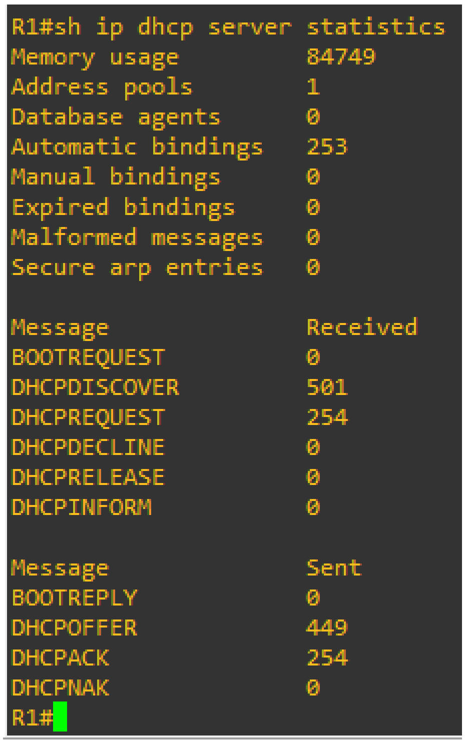
Maintenant le routeur ne peut plus répondre.
Stoppez l'attaque et vérifier le comportement du serveur DHCP via les commandes:

Router#show ip dhcp binding



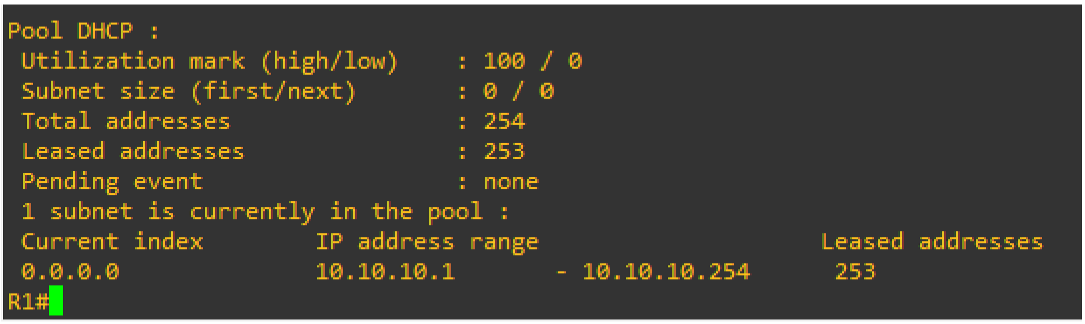
```
R1#sh ip dhcp binding
Bindings from all pools not associated with VRF:
IP address          Client-ID/              Lease expiration        Type
                    Hardware address/
                    User name
10.10.10.2          0100.0c29.7cb1.47       Oct 21 2024 02:38 PM    Automatic
10.10.10.3          0100.0c29.c283.52       Oct 21 2024 02:56 PM    Automatic
10.10.10.4          0016.3669.54e2          Oct 21 2024 02:57 PM    Automatic
10.10.10.5          0016.36f4.855c          Oct 21 2024 02:57 PM    Automatic
10.10.10.6          0016.3601.bd40          Oct 21 2024 02:57 PM    Automatic
10.10.10.7          0016.36c0.735a          Oct 21 2024 02:57 PM    Automatic
10.10.10.8          0016.36da.f558          Oct 21 2024 02:57 PM    Automatic
10.10.10.9          0016.3649.3719          Oct 21 2024 02:57 PM    Automatic
10.10.10.10         0016.3622.4e01          Oct 21 2024 02:57 PM    Automatic
10.10.10.11         0016.360a.9940          Oct 21 2024 02:58 PM    Automatic
10.10.10.12         0016.368a.f06f          Oct 21 2024 02:58 PM    Automatic
10.10.10.13         0016.36ae.0cf1          Oct 21 2024 02:58 PM    Automatic
10.10.10.14         0016.36c3.f9e7          Oct 21 2024 02:58 PM    Automatic
10.10.10.15         0016.3609.43e9          Oct 21 2024 02:58 PM    Automatic
10.10.10.16         0016.3604.b0b3          Oct 21 2024 02:58 PM    Automatic
10.10.10.17         0016.3677.0d57          Oct 21 2024 02:58 PM    Automatic
10.10.10.18         0016.3601.cc55          Oct 21 2024 02:58 PM    Automatic
10.10.10.19         0016.36be.dad7          Oct 21 2024 02:58 PM    Automatic
10.10.10.20         0016.3668.78e4          Oct 21 2024 02:58 PM    Automatic
10.10.10.21         0016.36a7.ae01          Oct 21 2024 02:58 PM    Automatic
10.10.10.22         0016.36a1.161b          Oct 21 2024 02:58 PM    Automatic
10.10.10.23         0016.367b.23fb          Oct 21 2024 02:58 PM    Automatic
10.10.10.24         0016.364f.4642          Oct 21 2024 02:58 PM    Automatic
10.10.10.25         0016.3695.edeb          Oct 21 2024 02:58 PM    Automatic
10.10.10.26         0016.3616.4d48          Oct 21 2024 02:58 PM    Automatic
10.10.10.27         0016.36a1.b681          Oct 21 2024 02:58 PM    Automatic
10.10.10.28         0016.36b8.6be0          Oct 21 2024 02:58 PM    Automatic
10.10.10.29         0016.369d.e2ed          Oct 21 2024 02:58 PM    Automatic
10.10.10.30         0016.3668.7b00          Oct 21 2024 02:58 PM    Automatic
10.10.10.31         0016.3689.52d9          Oct 21 2024 02:58 PM    Automatic
10.10.10.32         0016.3653.e133          Oct 21 2024 02:58 PM    Automatic
```

Router#show ip dhcp server statistics



```
R1#sh ip dhcp server statistics
Memory usage          84749
Address pools         1
Database agents       0
Automatic bindings    253
Manual bindings       0
Expired bindings      0
Malformed messages    0
Secure arp entries    0

Message               Received
BOOTREQUEST           0
DHCPDISCOVER          501
DHCPREQUEST           254
DHCPDECLINE           0
DHCPRELEASE           0
DHCPINFORM            0

Message               Sent
BOOTREPLY             0
DHCPOFFER             449
DHCPACK               254
DHCPNAK               0
R1#
```

Router#show ip dhcp pool

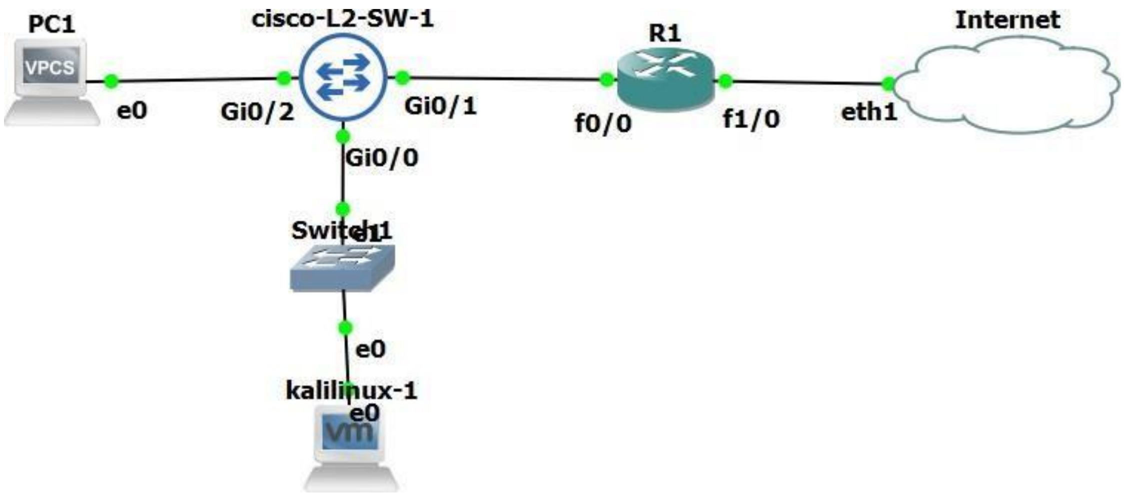


```
Pool DHCP :
 Utilization mark (high/low)    : 100 / 0
 Subnet size (first/next)       : 0 / 0
 Total addresses                : 254
 Leased addresses               : 253
 Pending event                  : none
 1 subnet is currently in the pool :
 Current index        IP address range                    Leased addresses
 0.0.0.0              10.10.10.1       - 10.10.10.254      253
R1#
```

TP 4.3 : DHCP snooping

Architecture réseau

- Un Routeur Cisco
- Un L2 Switch
- Un VPC
- VM Kali (PC Hacker)



Les étapes du TP :

- ouvrir l'émulateur GNS3
- sélectionner un routeur (serveur DHCP)
- sélectionner la machine kali linux (pc hacker) qui est déjà importée à l'émulateur.
- Lier les deux équipements avec un câble Ethernet
- Démarrer tous les équipements.

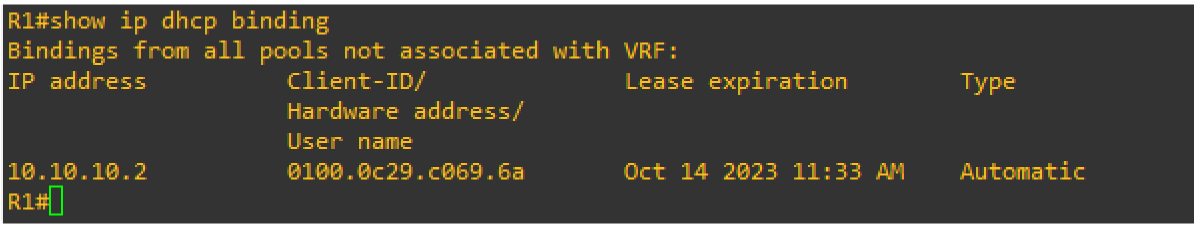
La Configuration du routeur

```
Router#conf t
Router(config)#interface fastEthernet 0/0
Router(config-if)# ip address 10.10.10.1 255.255.255.0
Router(config-if)#no shutdown
```

Router(config-if)#exit

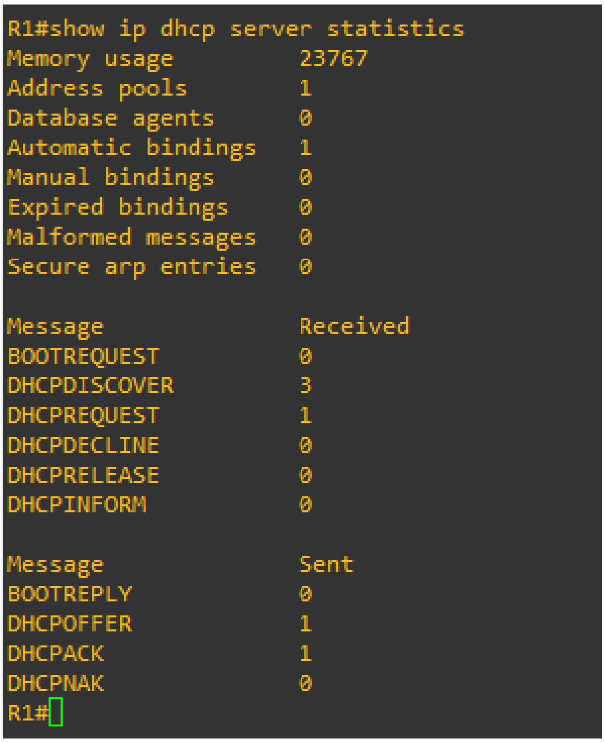
Activation du serveur DHCP

Router(config)# ip dhcp pool dhcp-tp
Router(dhcp-config)# network 10.10.10.0 255.255.255.0
Router(dhcp-config)# dns-server 8.8.8.8
Router(dhcp-config)# default-router 10.10.10.1
Router(config-if)#exit
Router(config)# exit
Router#show ip dhcp binding

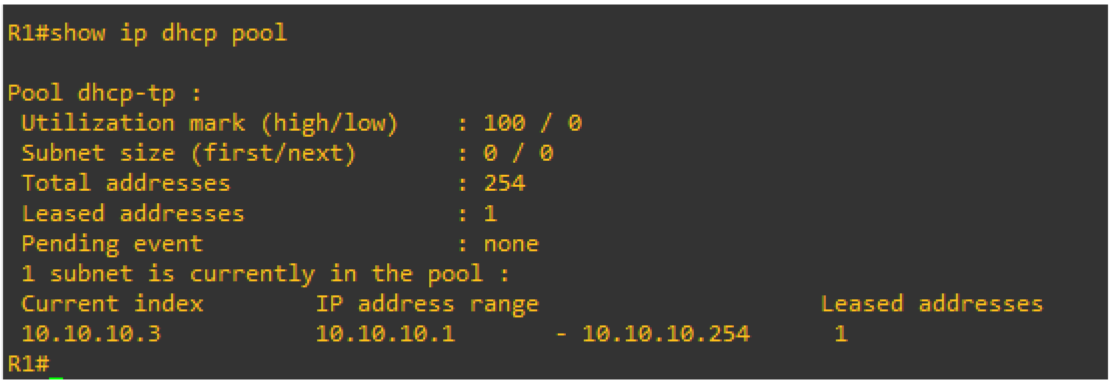


```
R1#show ip dhcp binding
Bindings from all pools not associated with VRF:
IP address          Client-ID/              Lease expiration        Type
                    Hardware address/
                    User name
10.10.10.2          0100.0c29.c069.6a       Oct 14 2023 11:33 AM    Automatic
R1#
```

Router#show ip dhcp server statistics

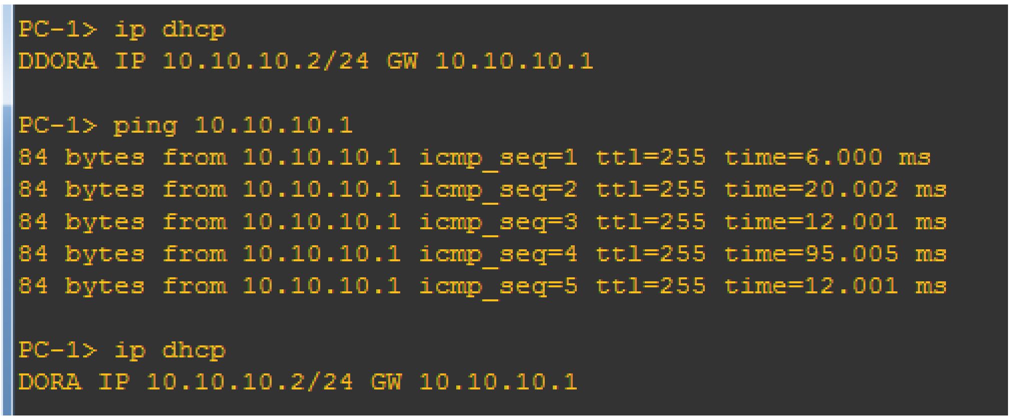


```
R1#show ip dhcp server statistics
Memory usage          23767
Address pools         1
Database agents       0
Automatic bindings    1
Manual bindings       0
Expired bindings      0
Malformed messages    0
Secure arp entries    0

Message               Received
BOOTREQUEST           0
DHCPDISCOVER          3
DHCPREQUEST           1
DHCPDECLINE           0
DHCPRELEASE           0
DHCPINFORM            0

Message               Sent
BOOTREPLY             0
DHCPOFFER             1
DHCPACK               1
DHCPNAK               0
R1#
```



```
R1#show ip dhcp pool

Pool dhcp-tp :
 Utilization mark (high/low)    : 100 / 0
 Subnet size (first/next)       : 0 / 0
 Total addresses                : 254
 Leased addresses               : 1
 Pending event                  : none
 1 subnet is currently in the pool :
 Current index        IP address range                    Leased addresses
 10.10.10.3           10.10.10.1       - 10.10.10.254      1
R1#
```

À partir du virtual PC, on va activer le DHCP et on va tester s'il va obtenir une adresse.



```
PC-1> ip dhcp
DDORA IP 10.10.10.2/24 GW 10.10.10.1

PC-1> ping 10.10.10.1
84 bytes from 10.10.10.1 icmp_seq=1 ttl=255 time=6.000 ms
84 bytes from 10.10.10.1 icmp_seq=2 ttl=255 time=20.002 ms
84 bytes from 10.10.10.1 icmp_seq=3 ttl=255 time=12.001 ms
84 bytes from 10.10.10.1 icmp_seq=4 ttl=255 time=95.005 ms
84 bytes from 10.10.10.1 icmp_seq=5 ttl=255 time=12.001 ms

PC-1> ip dhcp
DORA IP 10.10.10.2/24 GW 10.10.10.1
```

Activation de DHCP snooping sur le switcheur

Switch(config)# vlan 10

Switch(config)#interface gigabitEthernet0/0

Switch(config-if)#switchport mode access

Switch(config-if)#switchport access vlan 10

Switch(config-if)#exit

Switch(config)#interface gigabitEthernet0/1

Switch(config-if)#switchport mode access

Switch(config-if)#switchport access vlan 10

Switch(config-if)#exit

Switch(config)#interface gigabitEthernet 0/2

Switch(config-if)#switchport mode access

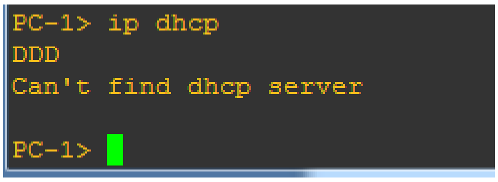
Switch(config-if)#switchport access vlan 10

Switch(config-if)#exit

Switch(config)#ip dhcp snooping

Switch(config)#ip dhcp snooping vlan 10

Tester de nouveau à partir d'une machine cliente :



```
PC-1> ip dhcp
DDD
Can't find dhcp server

PC-1>
```

Le VPC ne peut pas avoir une adresse ip via le serveur DHCP

Ajouter le port du serveur DHCP en tant que trusted port

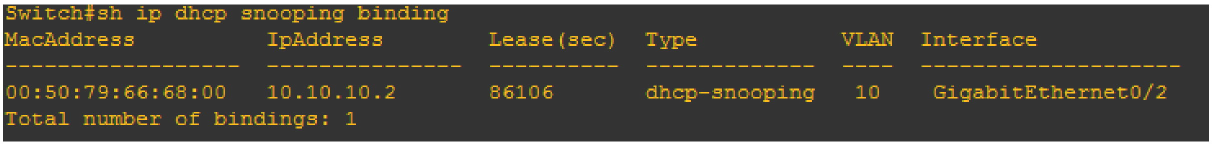
Switch(config)#interface gigabitEthernet 0/1

Switch(config-if)#ip dhcp snooping trust

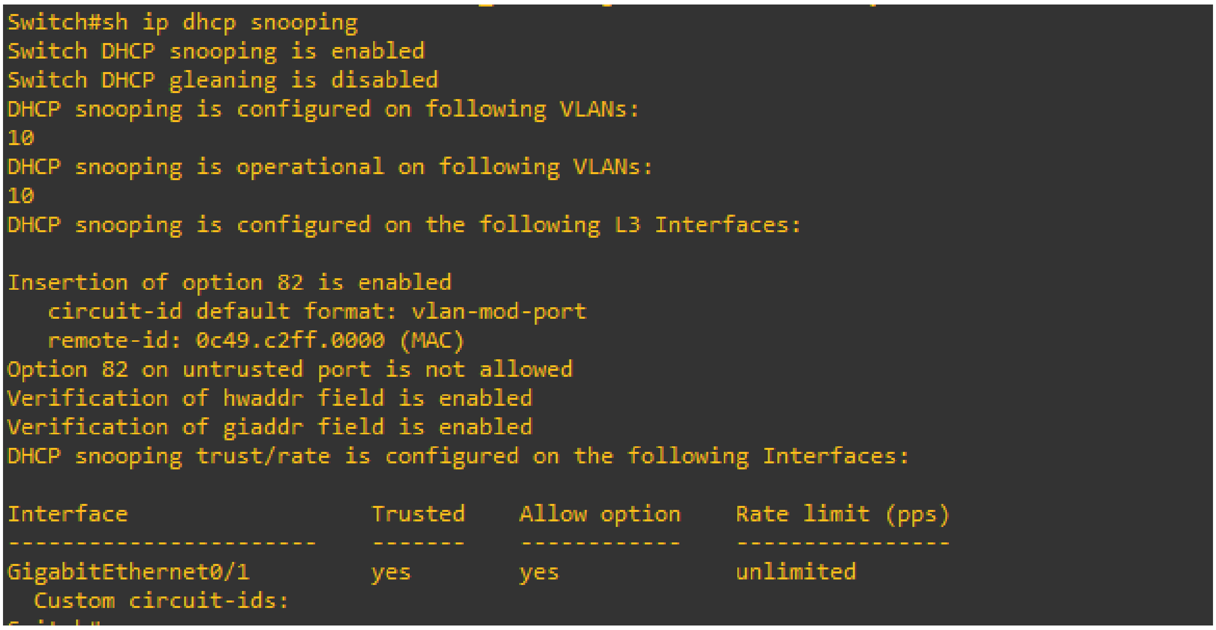
R1(config)#ip dhcp relay information trust-all

On va activer le DHCP et on va vérifier que la machine cliente va obtenir une adresse

Switch#sh ip dhcp snooping



```
Switch#sh ip dhcp snooping binding
MacAddress          IpAddress        Lease(sec)  Type           VLAN  Interface
------------------  ---------------  ----------  -------------  ----  --------------------
00:50:79:66:68:00   10.10.10.2       86106       dhcp-snooping   10    GigabitEthernet0/2
Total number of bindings: 1
```



```
Switch#sh ip dhcp snooping
Switch DHCP snooping is enabled
Switch DHCP gleaning is disabled
DHCP snooping is configured on following VLANs:
10
DHCP snooping is operational on following VLANs:
10
DHCP snooping is configured on the following L3 Interfaces:

Insertion of option 82 is enabled
   circuit-id default format: vlan-mod-port
   remote-id: 0c49.c2ff.0000 (MAC)
Option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled
Verification of giaddr field is enabled
DHCP snooping trust/rate is configured on the following Interfaces:

Interface                  Trusted    Allow option    Rate limit (pps)
-----------------------    -------    ------------    ----------------
GigabitEthernet0/1         yes        yes             unlimited
  Custom circuit-ids:
```