TP 1 - Remise dans le bain

Combien y a-t-il d'adresses disponibles dans un `/24` ?

254

Combien y a-t-il d'adresses disponibles dans un `/30` ?

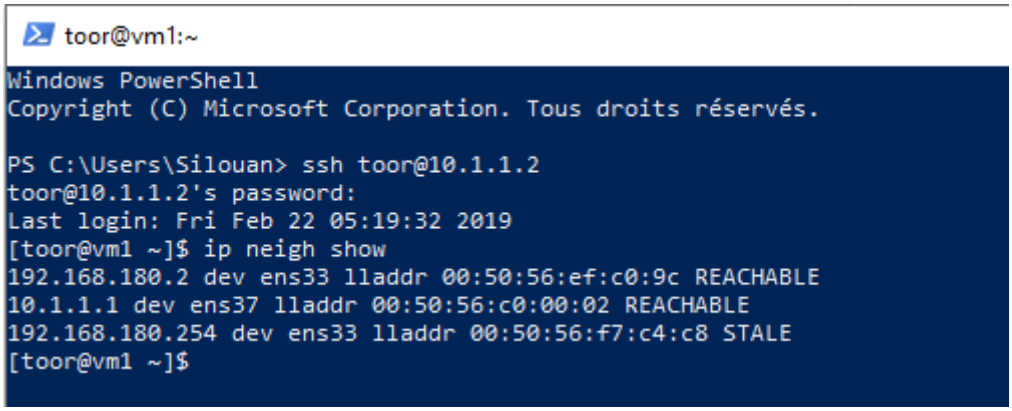
2

Il permet d'avoir 4 adresses dont deux utilisables, soit-on peu faire un réseau de deux machines

Table ARP

`ip neigh show` :

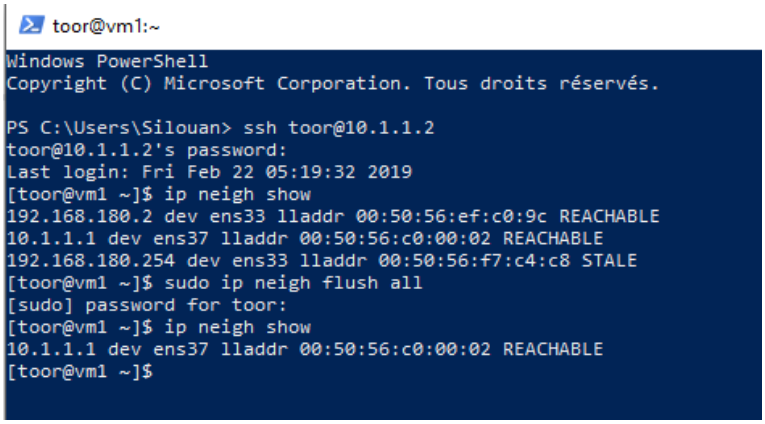
On affiche les voisins à notre ip



Vider la table ARP :

`sudo ip neigh flush all`

`ip neigh show`



Le Cossec Silouan feat Florent Nicolas

On re ping l'hôte:

toor@vm1:~

```
[toor@vm1 ~]$ ip neigh show
192.168.180.2 dev ens33 lladdr 00:50:56:ef:c0:9c REACHABLE
10.1.1.1 dev ens37 lladdr 00:50:56:c0:00:02 REACHABLE
[toor@vm1 ~]$ sudo ip neigh flush all
[toor@vm1 ~]$ ip neigh show
10.1.1.1 dev ens37 lladdr 00:50:56:c0:00:02 REACHABLE
[toor@vm1 ~]$ ping 10.1.2.2
PING 10.1.2.2 (10.1.2.2) 56(84) bytes of data.
64 bytes from 10.1.2.2: icmp_seq=1 ttl=128 time=0.840 ms
64 bytes from 10.1.2.2: icmp_seq=2 ttl=128 time=1.36 ms
^C
--- 10.1.2.2 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1000ms
rtt min/avg/max/mdev = 0.840/1.101/1.362/0.261 ms
[toor@vm1 ~]$ ip neigh show
192.168.180.2 dev ens33 lladdr 00:50:56:ef:c0:9c REACHABLE
10.1.1.1 dev ens37 lladdr 00:50:56:c0:00:02 REACHABLE
[toor@vm1 ~]$
```

On peut voir que le 192.168.180.2 est réapparut qui est l'ip de mon adaptater vmWare.

Capture réseau

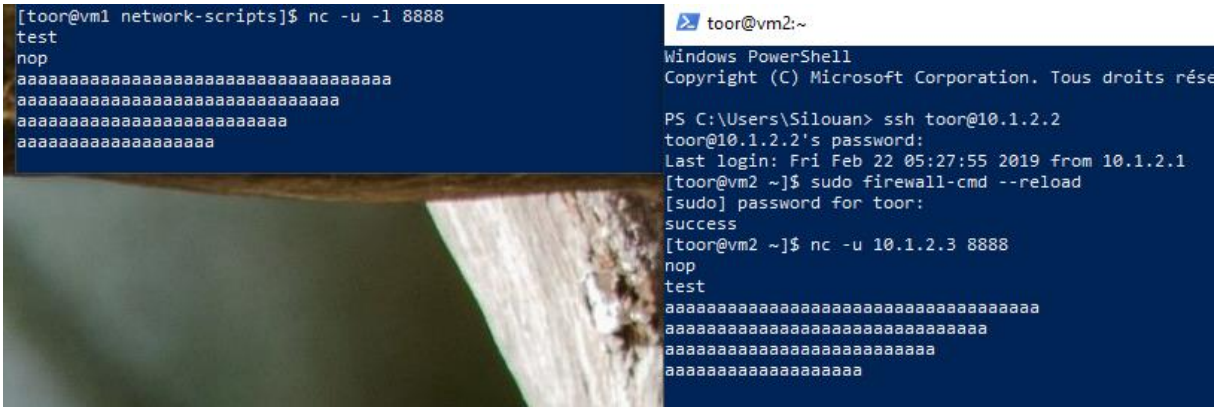
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	Vmware_c0:00:08	Broadcast	ARP	60	Who has 192.168.180.2? Tell 192.168.180.1
2	0.999963	Vmware_c0:00:08	Broadcast	ARP	60	Who has 192.168.180.2? Tell 192.168.180.1
3	3.656978	192.168.180.129	192.168.0.16	ICMP	98	Echo (ping) request id=0x26aa, seq=1/256, ttl=64 (reply in 4)
4	3.657782	192.168.0.16	192.168.180.129	ICMP	98	Echo (ping) reply id=0x26aa, seq=1/256, ttl=128 (request in 3)
5	4.658482	192.168.180.129	192.168.0.16	ICMP	98	Echo (ping) request id=0x26aa, seq=2/512, ttl=64 (reply in 6)
6	4.659395	192.168.0.16	192.168.180.129	ICMP	98	Echo (ping) reply id=0x26aa, seq=2/512, ttl=128 (request in 5)
7	5.660762	192.168.180.129	192.168.0.16	ICMP	98	Echo (ping) request id=0x26aa, seq=3/768, ttl=64 (reply in 8)
8	5.661760	192.168.0.16	192.168.180.129	ICMP	98	Echo (ping) reply id=0x26aa, seq=3/768, ttl=128 (request in 7)
9	6.662673	192.168.180.129	192.168.0.16	ICMP	98	Echo (ping) request id=0x26aa, seq=4/1024, ttl=64 (reply in 10)
10	6.663713	192.168.0.16	192.168.180.129	ICMP	98	Echo (ping) reply id=0x26aa, seq=4/1024, ttl=128 (request in 9)
11	8.665589	Vmware_7b:15:ef	Vmware_ef:c0:9c	ARP	42	Who has 192.168.180.2? Tell 192.168.180.129
12	8.665781	Vmware_ef:c0:9c	Vmware_7b:15:ef	ARP	60	192.168.180.2 is at 00:50:56:ef:c0:9c

II. Communication simple entre deux machines

Paquet ping2 :

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	Vmware_7b:15:03	Broadcast	ARP	60	Who has 10.1.2.2? Tell 10.1.2.3
2	0.000020	Vmware_5f:7a:2b	Vmware_7b:15:03	ARP	42	10.1.2.2 is at 00:0c:29:5f:7a:2b
3	0.000445	10.1.2.3	10.1.2.2	ICMP	98	Echo (ping) request id=0x1cdc, seq=1/256, ttl=64 (reply in 4)
4	0.000499	10.1.2.2	10.1.2.3	ICMP	98	Echo (ping) reply id=0x1cdc, seq=1/256, ttl=64 (request in 3)
5	1.002338	10.1.2.3	10.1.2.2	ICMP	98	Echo (ping) request id=0x1cdc, seq=2/512, ttl=64 (reply in 6)
6	1.002408	10.1.2.2	10.1.2.3	ICMP	98	Echo (ping) reply id=0x1cdc, seq=2/512, ttl=64 (request in 5)
7	2.003849	10.1.2.3	10.1.2.2	ICMP	98	Echo (ping) request id=0x1cdc, seq=3/768, ttl=64 (reply in 8)
8	2.003909	10.1.2.2	10.1.2.3	ICMP	98	Echo (ping) reply id=0x1cdc, seq=3/768, ttl=64 (request in 7)
9	3.004739	10.1.2.3	10.1.2.2	ICMP	98	Echo (ping) request id=0x1cdc, seq=4/1024, ttl=64 (reply in 10)
10	3.004796	10.1.2.2	10.1.2.3	ICMP	98	Echo (ping) reply id=0x1cdc, seq=4/1024, ttl=64 (request in 9)
11	5.001078	Vmware_5f:7a:2b	Vmware_7b:15:03	ARP	42	Who has 10.1.2.3? Tell 10.1.2.2
12	5.001578	Vmware_7b:15:03	Vmware_5f:7a:2b	ARP	60	10.1.2.3 is at 00:0c:29:7b:15:03

Netcat :



Le petit ss des familles

```
[toor@vm1 ~]$ ss -unp
Recv-Q Send-Q                 Local Address:Port                                Peer Address:Port
0      0                          10.1.2.3:8888                                    10.1.2.2:43538
sers:(("nc",pid=8226,fd=4))
[toor@vm1 ~]$
```

On apllique le filtre udp sur wireshark :

udp

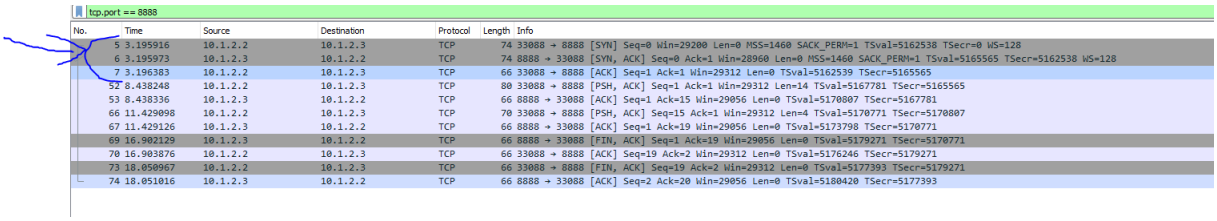
No.	Time	Source	Destination	Protocol	Length	Info
17	3.566188	10.1.2.2	10.1.2.3	UDP	60	43538 → 8888 Len=5
29	4.411684	10.1.2.2	10.1.2.3	UDP	60	43538 → 8888 Len=4
38	4.622799	10.1.2.2	10.1.2.3	UDP	60	43538 → 8888 Len=3
47	4.824283	10.1.2.2	10.1.2.3	UDP	60	43538 → 8888 Len=3
54	5.034575	10.1.2.2	10.1.2.3	UDP	60	43538 → 8888 Len=2

On peut même récupérer les messages transmis et on voit des paquet UDP en plus.

Tcp :

3-way handshake TCP :

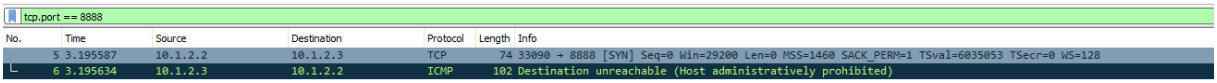
Le Cossec Silouan feat Florent Nicolas



tcp.port == 8888

No.	Time	Source	Destination	Protocol	Length	Info
5	3.195916	10.1.2.2	10.1.2.3	TCP	74	33088 → 8888 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=5162538 TSecr=0 WS=128
6	3.195973	10.1.2.3	10.1.2.2	TCP	74	8888 → 33088 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=5165565 TSecr=5162538 WS=128
7	3.196383	10.1.2.2	10.1.2.3	TCP	66	33088 → 8888 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=5162539 TSecr=5165565
52	8.438248	10.1.2.2	10.1.2.3	TCP	80	33088 → 8888 [PSH, ACK] Seq=1 Ack=1 Win=29312 Len=14 TSval=5167781 TSecr=5165565
53	8.438336	10.1.2.3	10.1.2.2	TCP	66	8888 → 33088 [ACK] Seq=1 Ack=15 Win=29056 Len=0 TSval=5170807 TSecr=5167781
66	11.429098	10.1.2.2	10.1.2.3	TCP	70	33088 → 8888 [PSH, ACK] Seq=15 Ack=1 Win=29312 Len=4 TSval=5170771 TSecr=5170807
67	11.429126	10.1.2.3	10.1.2.2	TCP	66	8888 → 33088 [ACK] Seq=1 Ack=19 Win=29056 Len=0 TSval=5173798 TSecr=5170771
69	16.902129	10.1.2.3	10.1.2.2	TCP	66	8888 → 33088 [FIN, ACK] Seq=1 Ack=19 Win=29056 Len=0 TSval=5179271 TSecr=5170771
70	16.903876	10.1.2.2	10.1.2.3	TCP	66	33088 → 8888 [ACK] Seq=19 Ack=2 Win=29312 Len=0 TSval=5176246 TSecr=5179271
73	18.050967	10.1.2.2	10.1.2.3	TCP	66	33088 → 8888 [FIN, ACK] Seq=19 Ack=2 Win=29312 Len=0 TSval=5177393 TSecr=5179271
74	18.051016	10.1.2.3	10.1.2.2	TCP	66	8888 → 33088 [ACK] Seq=2 Ack=20 Win=29056 Len=0 TSval=5180420 TSecr=5177393

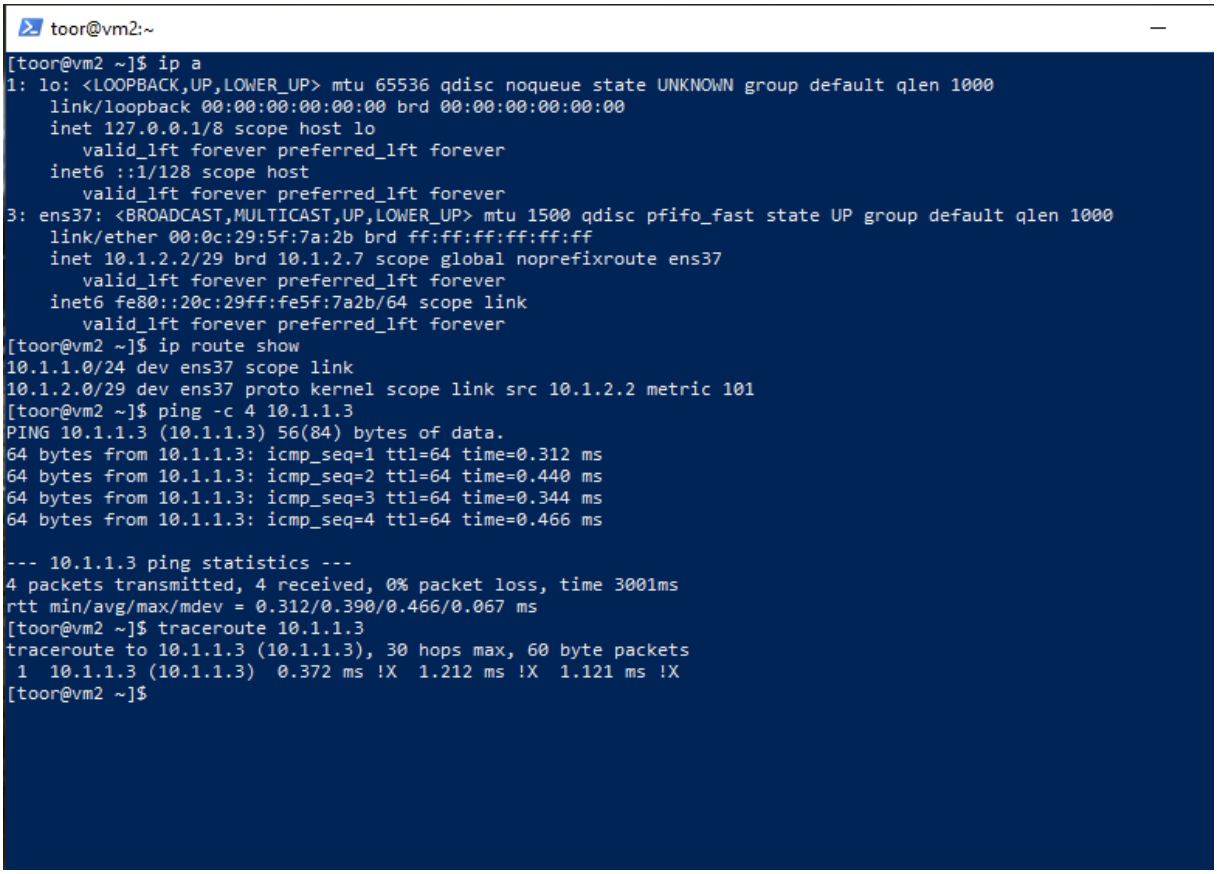
On enlève la règle du pare-feu :



tcp.port == 8888

No.	Time	Source	Destination	Protocol	Length	Info
5	3.195587	10.1.2.2	10.1.2.3	TCP	74	33090 → 8888 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=6035053 TSecr=0 WS=128
6	3.195634	10.1.2.3	10.1.2.2	ICMP	102	Destination unreachable (Host administratively prohibited)

III. Routage statique simple



toor@vm2:~

```
[toor@vm2 ~]$ 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
3: ens37: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:0c:29:5f:7a:2b brd ff:ff:ff:ff:ff:ff
    inet 10.1.2.2/29 brd 10.1.2.7 scope global noprefixroute ens37
       valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fe5f:7a2b/64 scope link
       valid_lft forever preferred_lft forever
[toor@vm2 ~]$ ip route show
10.1.1.0/24 dev ens37 scope link
10.1.2.0/29 dev ens37 proto kernel scope link src 10.1.2.2 metric 101
[toor@vm2 ~]$ ping -c 4 10.1.1.3
PING 10.1.1.3 (10.1.1.3) 56(84) bytes of data.
64 bytes from 10.1.1.3: icmp_seq=1 ttl=64 time=0.312 ms
64 bytes from 10.1.1.3: icmp_seq=2 ttl=64 time=0.440 ms
64 bytes from 10.1.1.3: icmp_seq=3 ttl=64 time=0.344 ms
64 bytes from 10.1.1.3: icmp_seq=4 ttl=64 time=0.466 ms

--- 10.1.1.3 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3001ms
rtt min/avg/max/mdev = 0.312/0.390/0.466/0.067 ms
[toor@vm2 ~]$ traceroute 10.1.1.3
traceroute to 10.1.1.3 (10.1.1.3), 30 hops max, 60 byte packets
 1  10.1.1.3 (10.1.1.3)  0.372 ms !X  1.212 ms !X  1.121 ms !X
[toor@vm2 ~]$
```