TP ARP

TP U6 SISR

SPINELLI Dylan
BTS SIO SISR | PARIS YNOV CAMPUS

Table des matières

1-Introduction au protocole ARP

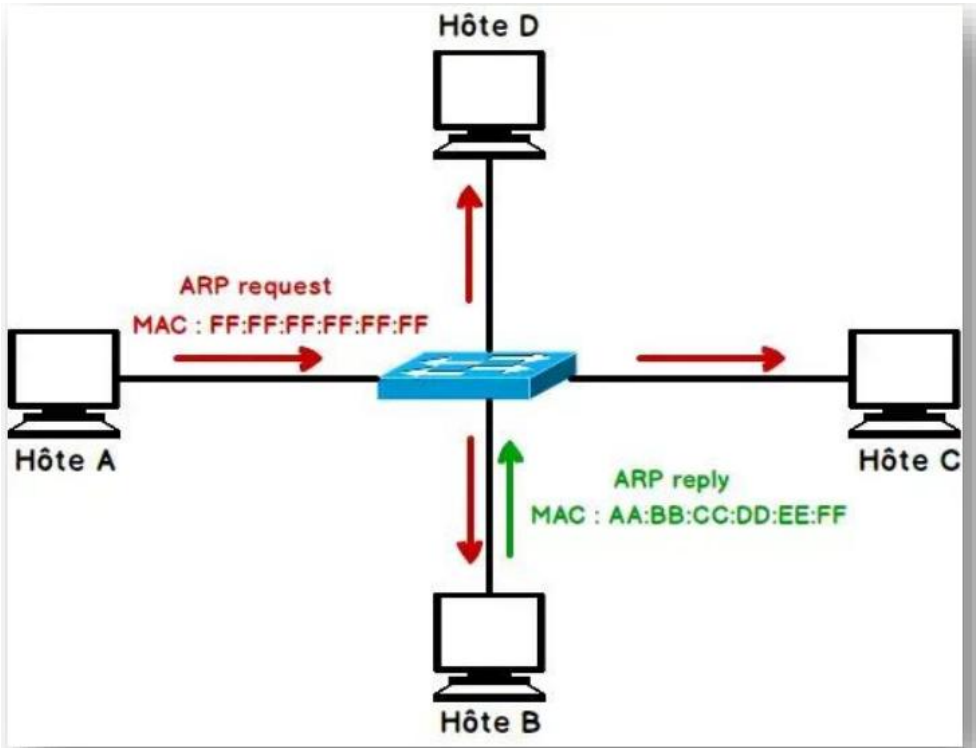
Le protocole **ARP** (*Address Resolution Protocol*) est un élément fondamental des réseaux informatiques. Son rôle principal est d'assurer la traduction entre une adresse logique de niveau 3 (l'adresse IP) et une adresse physique de niveau 2 (l'adresse MAC) du modèle OSI.

Concrètement, lorsqu'un équipement souhaite envoyer des données à une autre machine sur son réseau local, il connaît généralement son adresse IP, mais il a impérativement besoin de son adresse MAC pour construire la trame Ethernet. Le protocole ARP permet d'interroger le réseau via un message de diffusion (Broadcast) pour découvrir cette adresse MAC manquante.

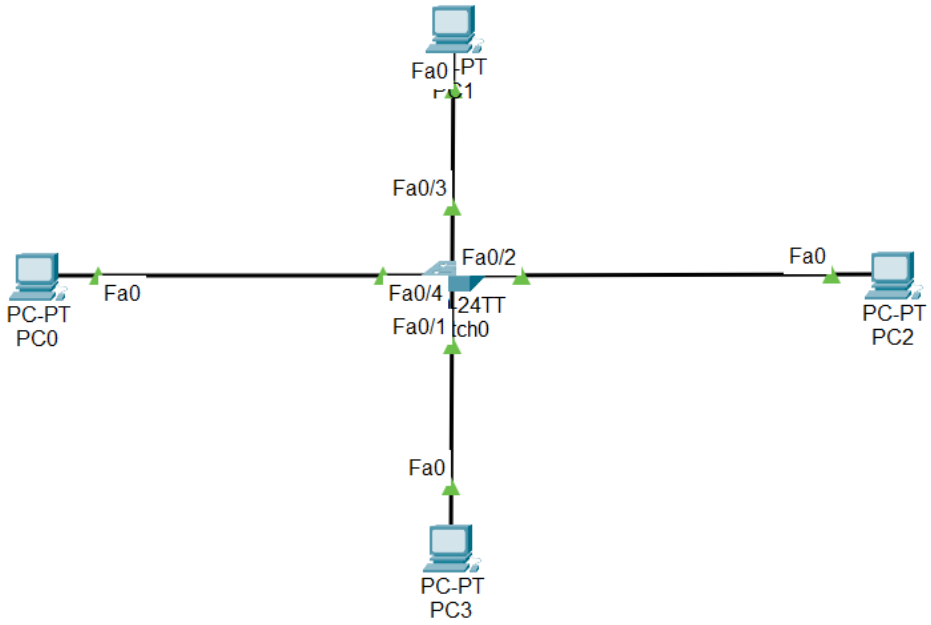
Ce compte-rendu a pour objectif d'illustrer le fonctionnement de ce protocole, d'abord à travers une simulation sur **Cisco Packet Tracer**, puis par l'analyse de trames réelles sur une machine virtuelle Debian à l'aide de l'outil **Wireshark**.

2- Réalisation de la maquette sur Cisco

Nous allons réaliser la maquette suivante sur cisco :

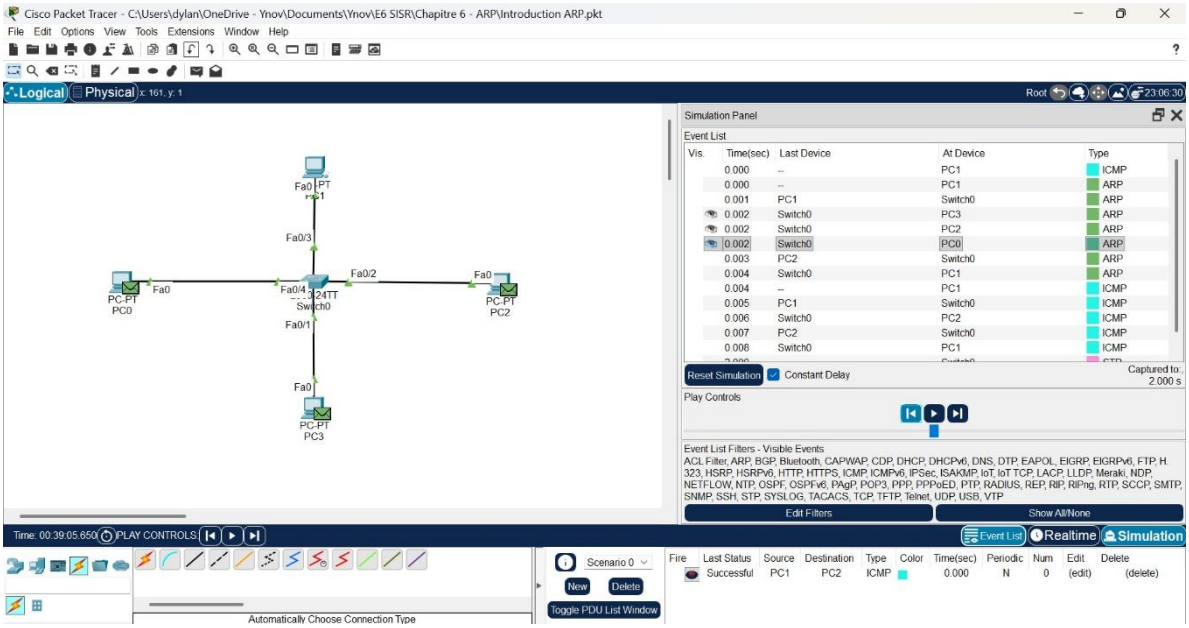


Voici la maquette réalisée dans Cisco :



3-Visualisation des requêtes ARP

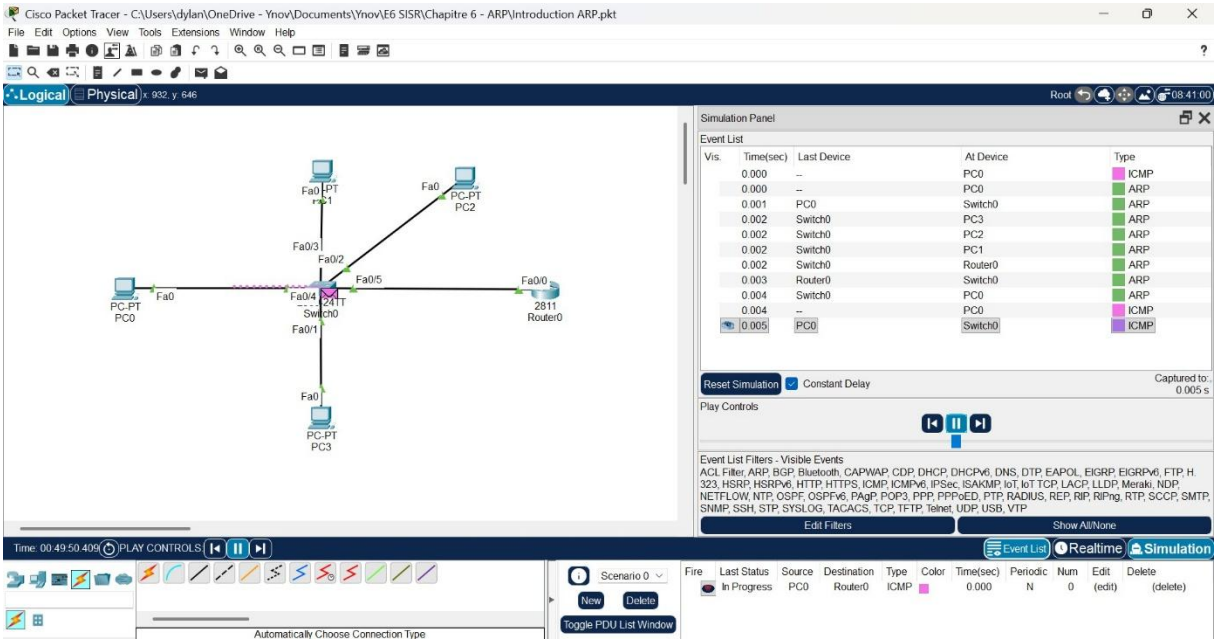
Faisons un ping entre PC1 et PC2 pour visualiser les requêtes ARP :



On constate que les requêtes ARP sont bien envoyées à tous les PC du réseau.

4-Test avec un routeur

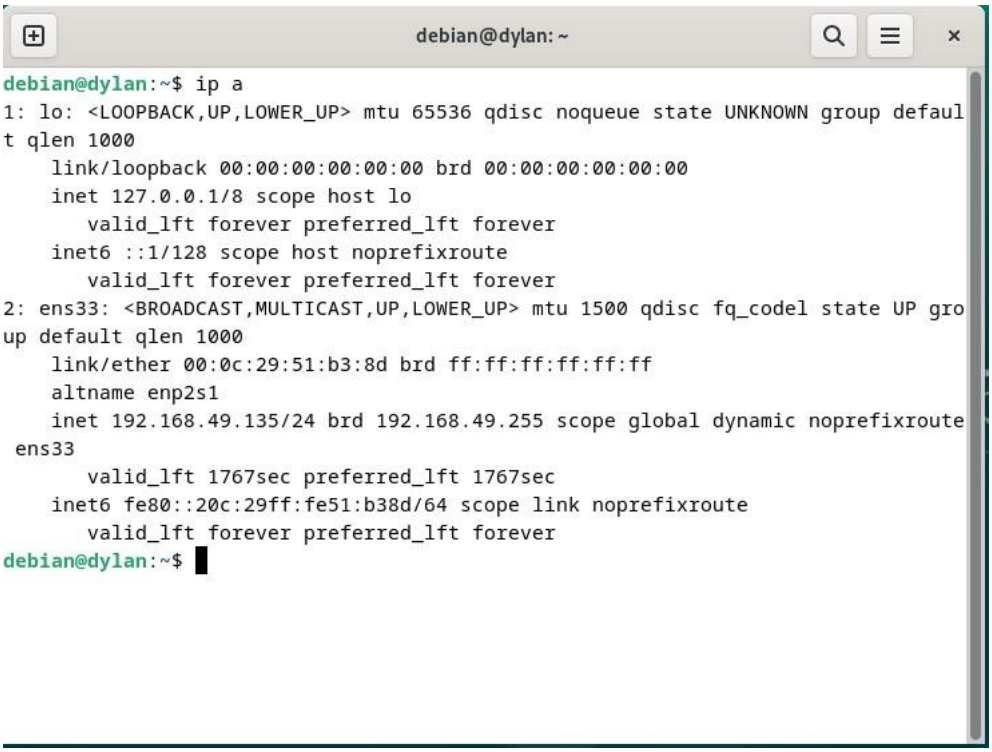
Faisons maintenant le test avec un routeur. On teste un ping de PC0 vers le routeur :

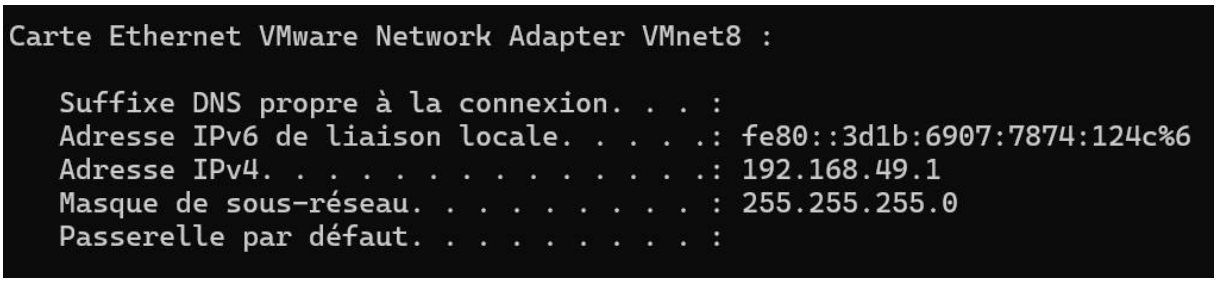


On constate que le routeur ne diffuse pas les requêtes ARP sur tous ses ports, contrairement au switch. En effet, le routeur bloque les requêtes de diffusion.

5-Observation des requêtes ARP sur Wireshark

On rappelle l'adresse IP de notre VM ainsi que celle du PC physique :

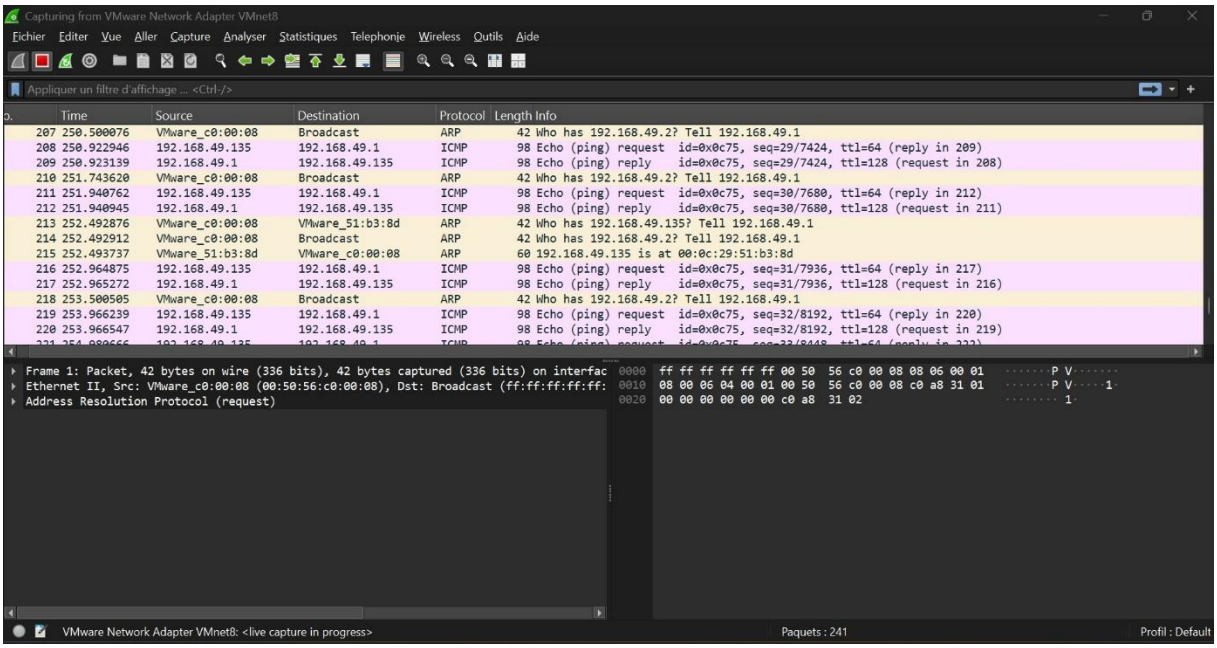




Voici la gateway de la VM :

```
debian@dylan: ~
debian@dylan:~$ ping 192.168.49.1
PING 192.168.49.1 (192.168.49.1) 56(84) bytes of data.
64 bytes from 192.168.49.1: icmp_seq=1 ttl=128 time=0.617 ms
64 bytes from 192.168.49.1: icmp_seq=2 ttl=128 time=0.959 ms
64 bytes from 192.168.49.1: icmp_seq=3 ttl=128 time=0.778 ms
64 bytes from 192.168.49.1: icmp_seq=4 ttl=128 time=1.01 ms
64 bytes from 192.168.49.1: icmp_seq=5 ttl=128 time=1.10 ms
64 bytes from 192.168.49.1: icmp_seq=6 ttl=128 time=1.29 ms
64 bytes from 192.168.49.1: icmp_seq=7 ttl=128 time=1.19 ms
^C
--- 192.168.49.1 ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6032ms
rtt min/avg/max/mdev = 0.617/0.994/1.294/0.217 ms
debian@dylan:~$ ip route show
default via 192.168.49.2 dev ens33 proto dhcp src 192.168.49.135 metric 100
192.168.49.0/24 dev ens33 proto kernel scope link src 192.168.49.135 metric 100
debian@dylan:~$ nano /etc/network/interfaces
debian@dylan:~$
```

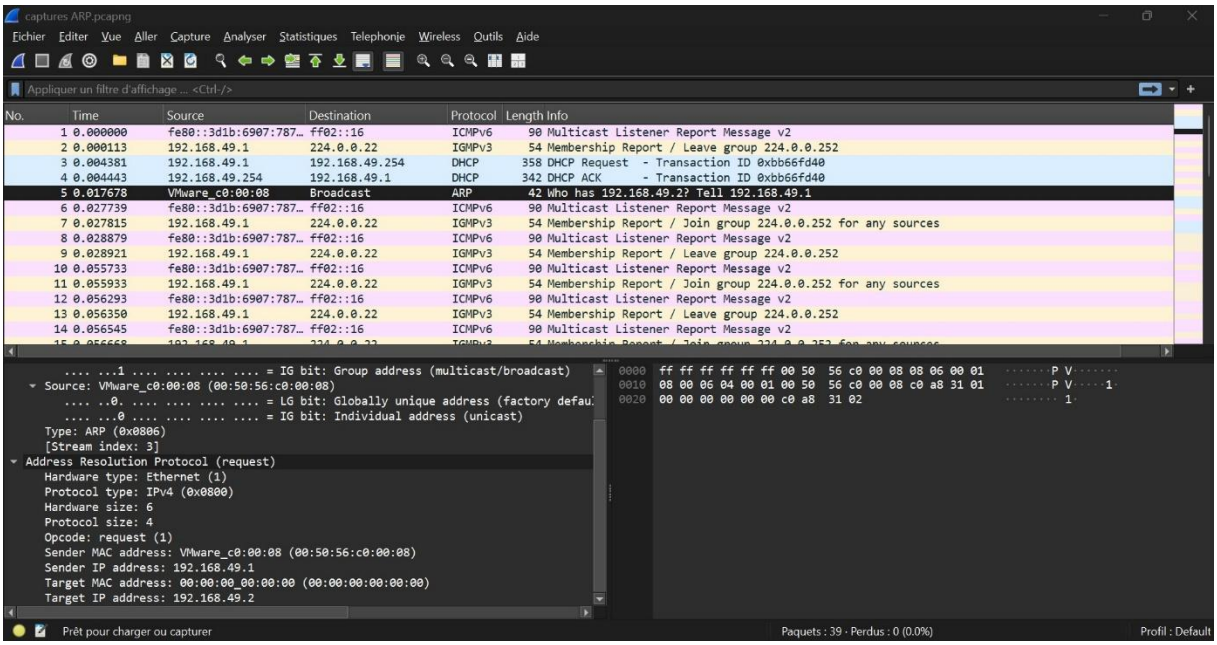
On peut observer les requêtes ARP sur wireshark :



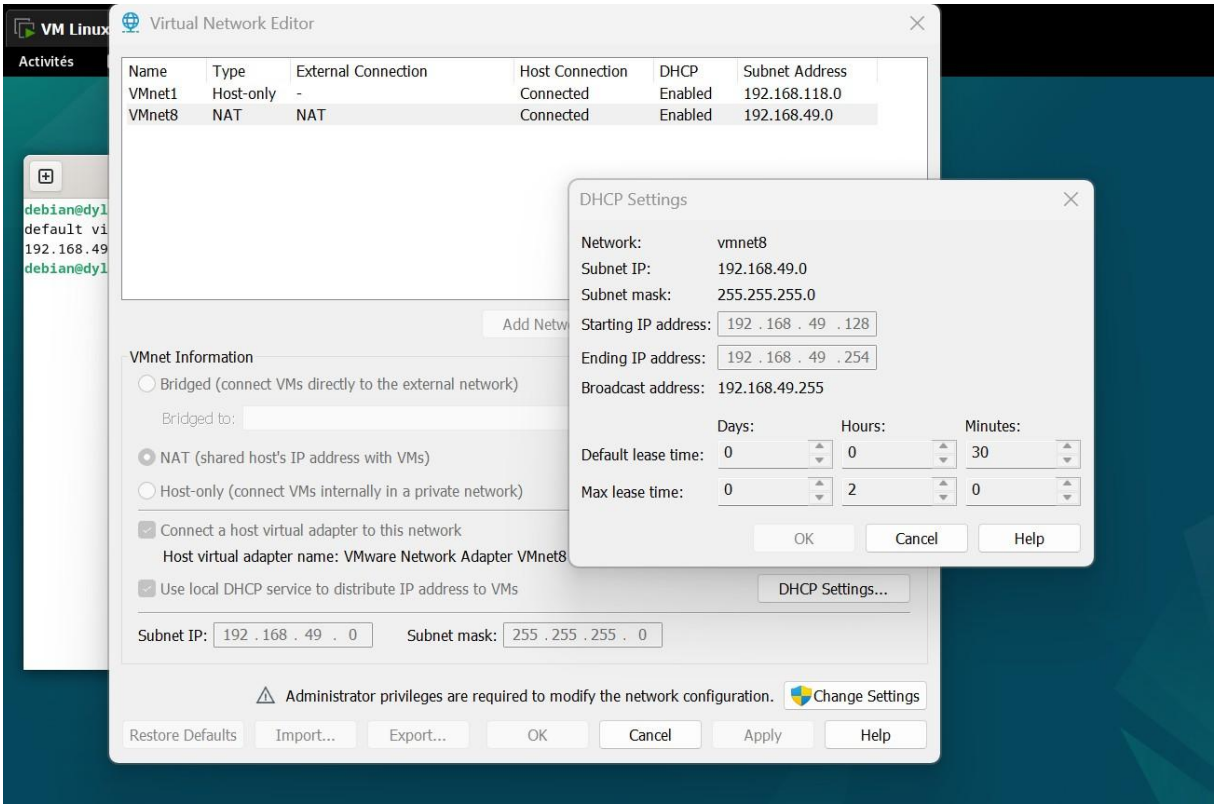
1. La requête (ARP Request - Ligne jaune) : On observe la trame « Who has 192.168.49.2? Tell 192.168.49.1 ». La machine hôte (.1) cherche l'adresse MAC de la passerelle NAT de VMware (.2). Dans les détails de la trame (en bas), on voit que l'adresse MAC de destination est ff:ff:ff:ff:ff:ff. C'est l'adresse de **Broadcast** (diffusion) : le message est envoyé à tout le réseau.

2. **Les pings (ICMP - Lignes roses) :** On observe ensuite des échanges "Echo request / Echo reply" entre notre VM (192.168.49.135) et l'hôte (192.168.49.1), prouvant que la communication bidirectionnelle fonctionne une fois les adresses MAC connues.

3. **La réponse (ARP Reply) :** Plus bas, on peut voir la VM informer le réseau de son adresse : « *192.168.49.135 is at 00:0c:29:51:b3:8d* ».



Vérification de la passerelle (Gateway) : > La commande ip route show tapée sur la VM Debian confirme que la route par défaut (default via) passe par 192.168.49.2. C'est l'adresse de la passerelle virtuelle créée par le service NAT de VMware.



Cette configuration est confirmée par le *Virtual Network Editor* de VMware, qui montre que le sous-réseau 192.168.49.0/24 est bien géré en NAT, ce qui permet à la VM de communiquer avec l'extérieur en utilisant l'adresse IP de la machine physique.