SIMULATION RESEAU ET ANALYSE DE TRAFIC AVEC GNS3 ET VMWARE

BTS S.I.O. OPTION S.I.S.R. -- 2025 - 2026

MR MICHELE MASTROGIACOMO

Introduction

Dans ce TP j'ai mise en place une simulation réseau à l'aide du logiciel GNS3.
L'objectif est de créer une communication entre deux machines en passant par un routeur Cisco IOSv v15.9(3)M6, puis d'analyser le trafic réseau à l'aide de Wireshark.

Ce TP permet de comprendre :

- le fonctionnement du routage
- la communication entre machines
- l'analyse des paquets réseau (ICMP et ARP)

Présentation de l'environnement

Les machines virtuelles utilisées dans ce TP sont hébergées via VMware, sauf Cisco.
Cet outil permet de créer et exécuter plusieurs systèmes d'exploitation sur un même ordinateur physique.
Il facilite la mise en place d'un environnement de test sans nécessiter de matériel réel, tout en étant compatible avec GNS3.

Dans ce TP, plusieurs outils ont été utilisés afin de mettre en place et analyser l'environnement réseau.

- GNS3 : permet de simuler une infrastructure réseau en reliant différents équipements virtuels.
- Cisco IOSv v15.9(3)M6: utilisé comme routeur afin d'assurer le routage entre les différents réseaux.
- Wireshark : permet de capturer et analyser les paquets réseau.
- VMware : utilisé pour héberger les machines virtuelles nécessaires au TP.
- Ubuntu Server

Ces outils permettent de reproduire un environnement réseau réaliste sans utiliser de matériel physique.

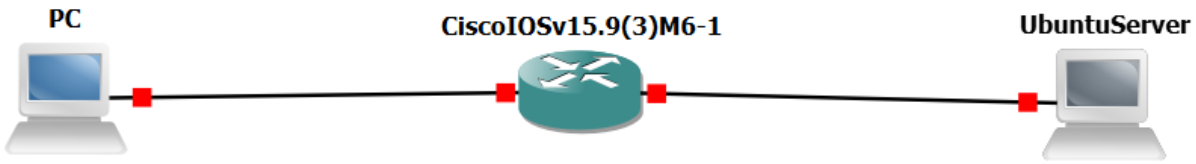
Architecture réseau

Dans ce TP, une architecture simple a été mise en place afin de tester la communication entre deux machines via un routeur.

Le réseau est composé de :

- un poste client (PC)
- un routeur Cisco IOSv v15.9(3)M6
- un serveur Ubuntu

Image 1 : Topologie GNS3 - Cette capture présente la topologie réseau utilisée dans GNS3. Elle montre les deux machines reliées au routeur, chacune dans un réseau différent.



Chaque machine appartient à un réseau différent :

Équipement	Adresse IP	Réseau
PC	192.168.2.10	192.168.2.0/24
Routeur (eth1)	192.168.2.1	
Routeur (eth2)	192.168.3.1	
Serveur	192.168.3.10	192.168.3.0/24

Mise en place

Configuration des machines

Les adresses IP ont été configurées sur chaque machine afin de permettre leur identification sur le réseau.

Image 2 : configuration IP PC client

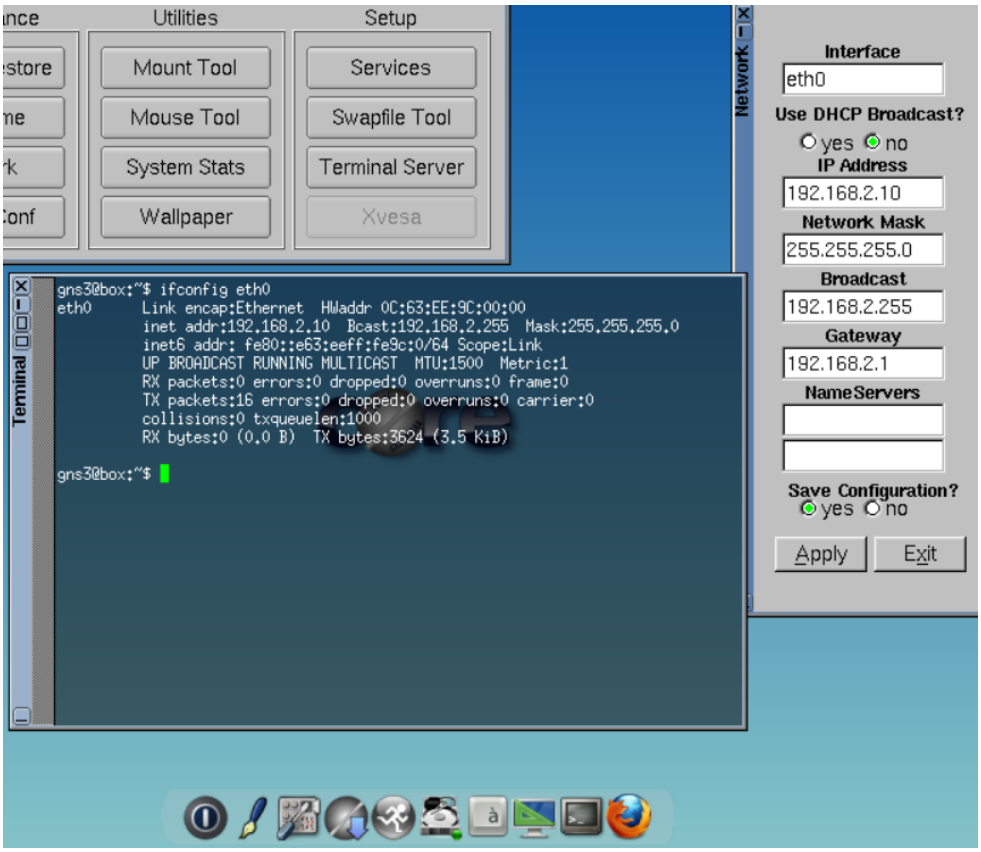


Image 3 : Installation Serveur Web Sur Machine Virtuelle VMWare

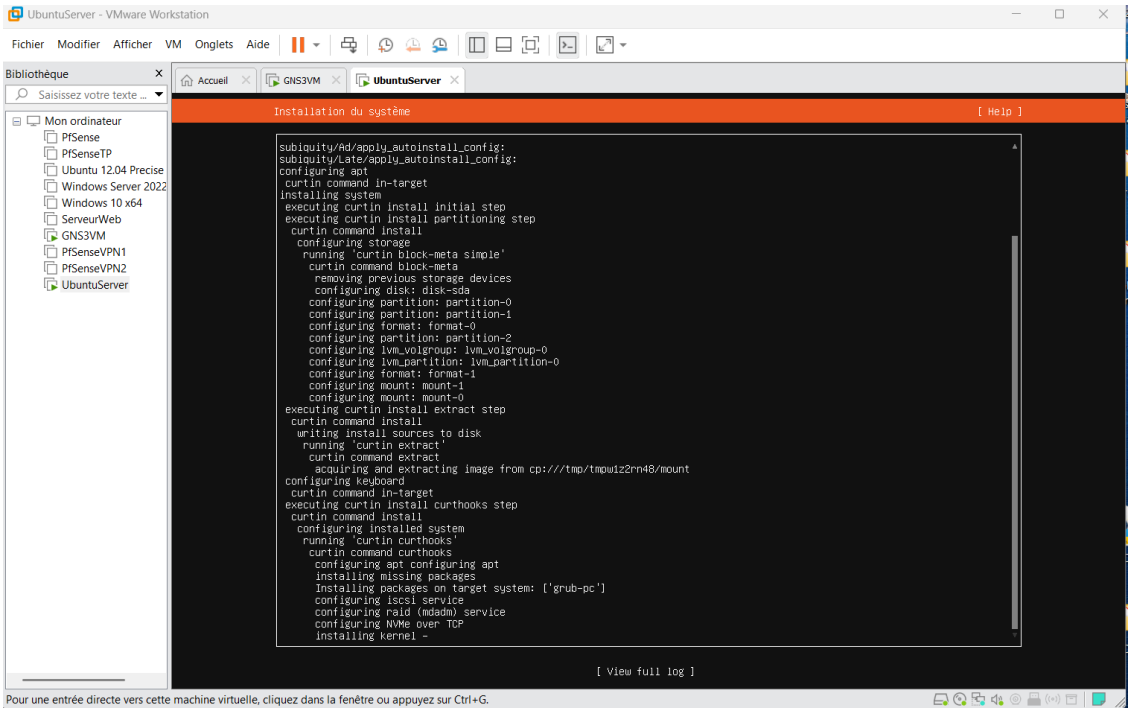
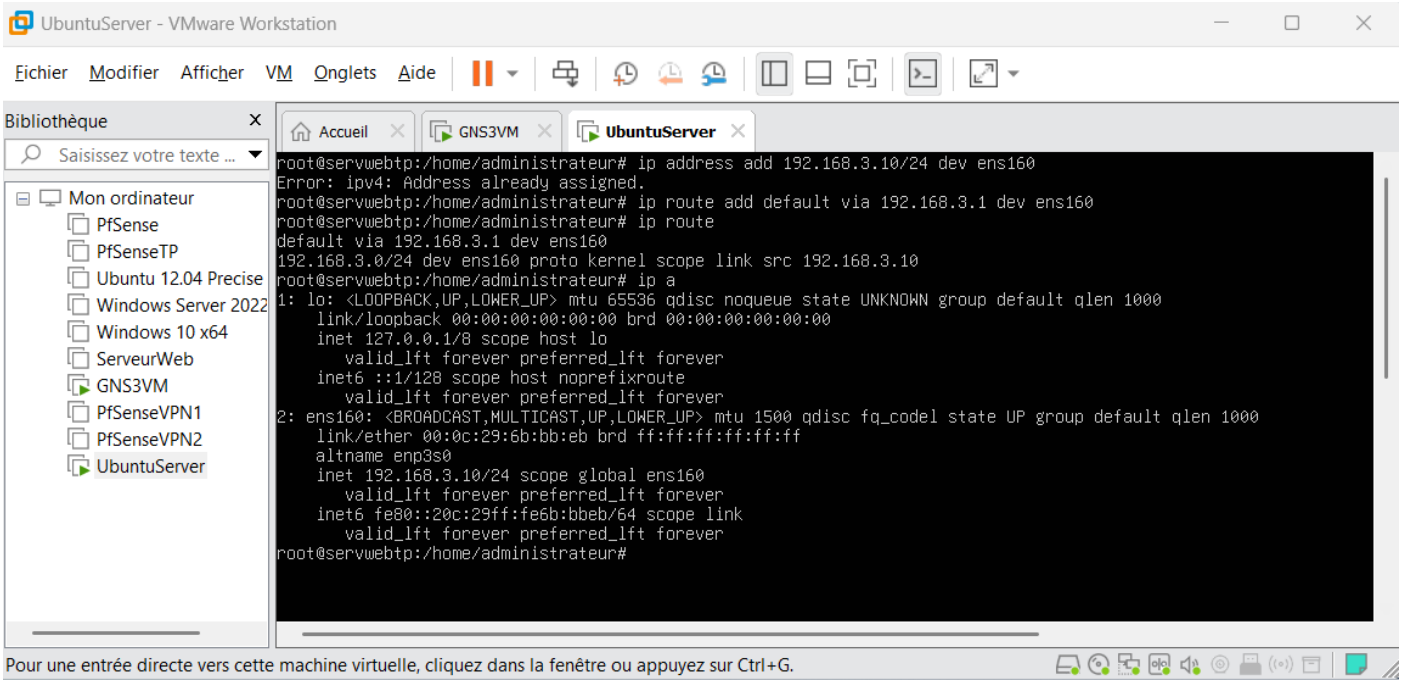


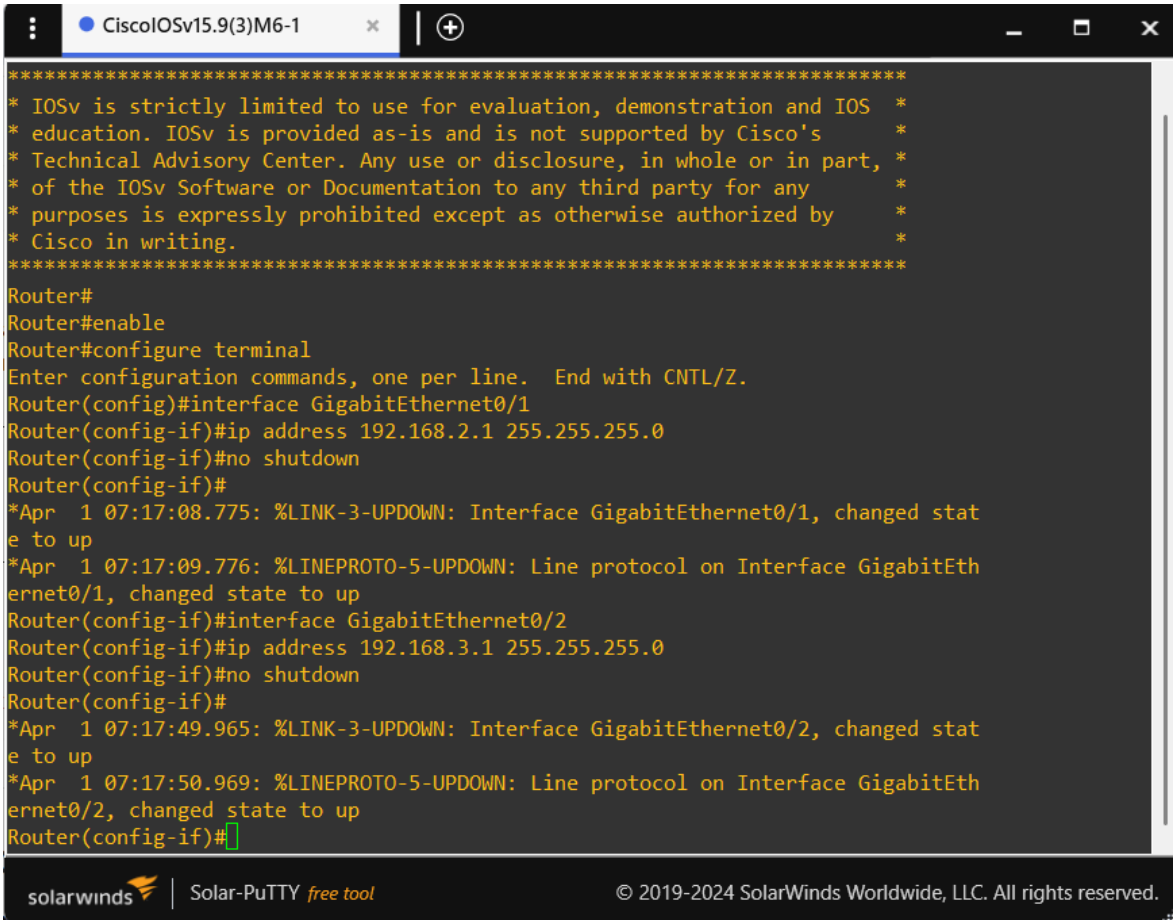
Image 4 : configuration IP Serveur



Configuration du routeur Cisco

Le routeur a été configuré avec deux interfaces réseau afin d'assurer la communication entre les deux réseaux.

Image 5 : Cette capture montre la configuration des interfaces du routeur Cisco, permettant de relier les deux réseaux et d'assurer le routage entre eux.

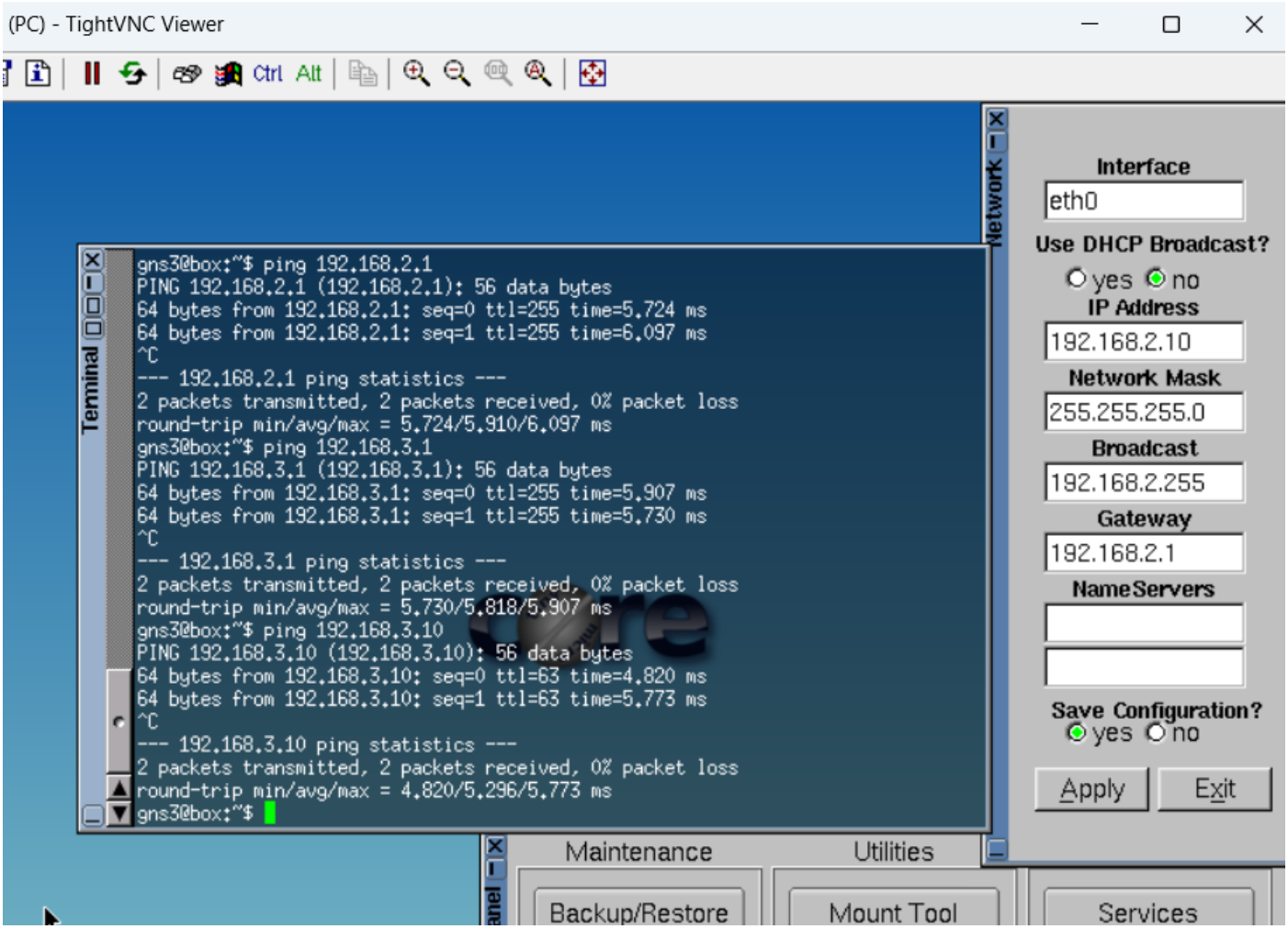


Tests de connectivité

Des tests ont été réalisés afin de vérifier la communication entre les équipements.

La commande ping a été utilisée pour tester la connexion entre le client , router et serveur.

Image 6 : ping du PC client vers le routeur et vers le serveur



Analyse du trafic

Une capture du trafic réseau a été effectuée avec Wireshark.

L'analyse a permis d'observer :

- les paquets ICMP (ping) pour test connectivité
- les échanges ARP

Image 7 : Cette capture montre le lancement de l'analyse réseau via Wireshark directement depuis GNS3 en sélectionnant un lien entre deux équipements.

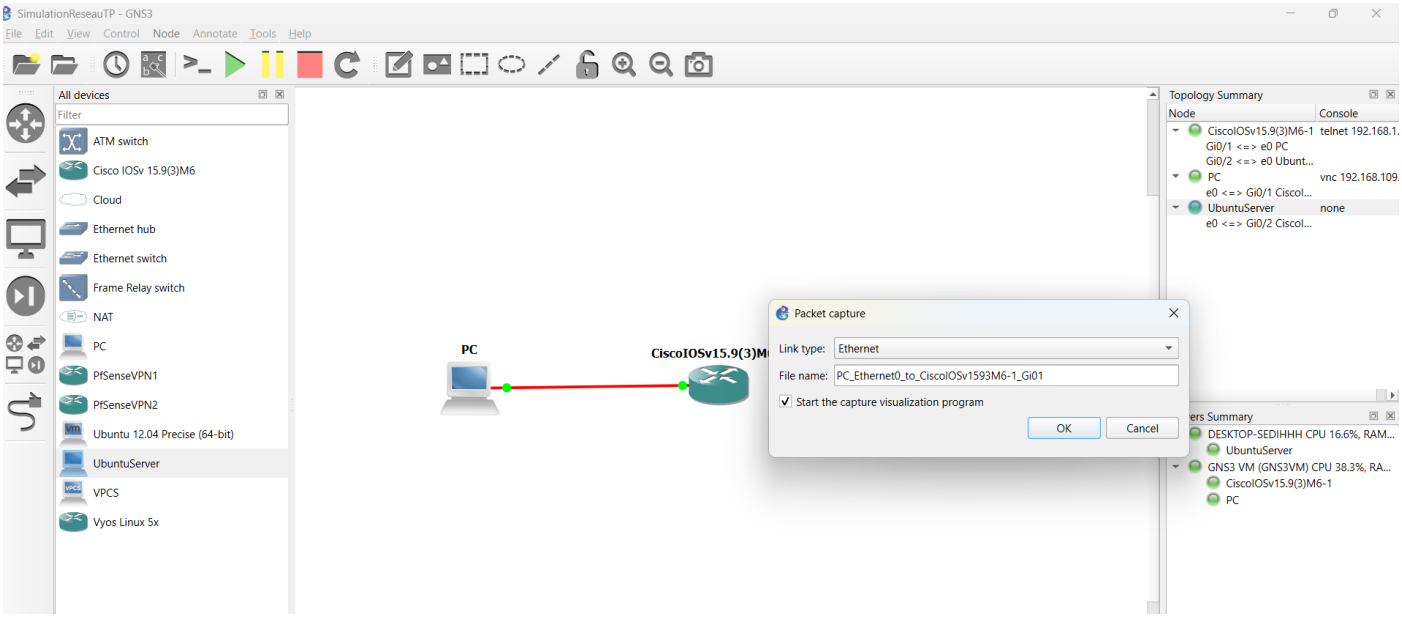


Image 8 : Cette capture montre les paquets ICMP échangés lors de l'exécution de la commande ping. On observe les requêtes (Echo Request) envoyées par le client et les réponses (Echo Reply) du serveur.

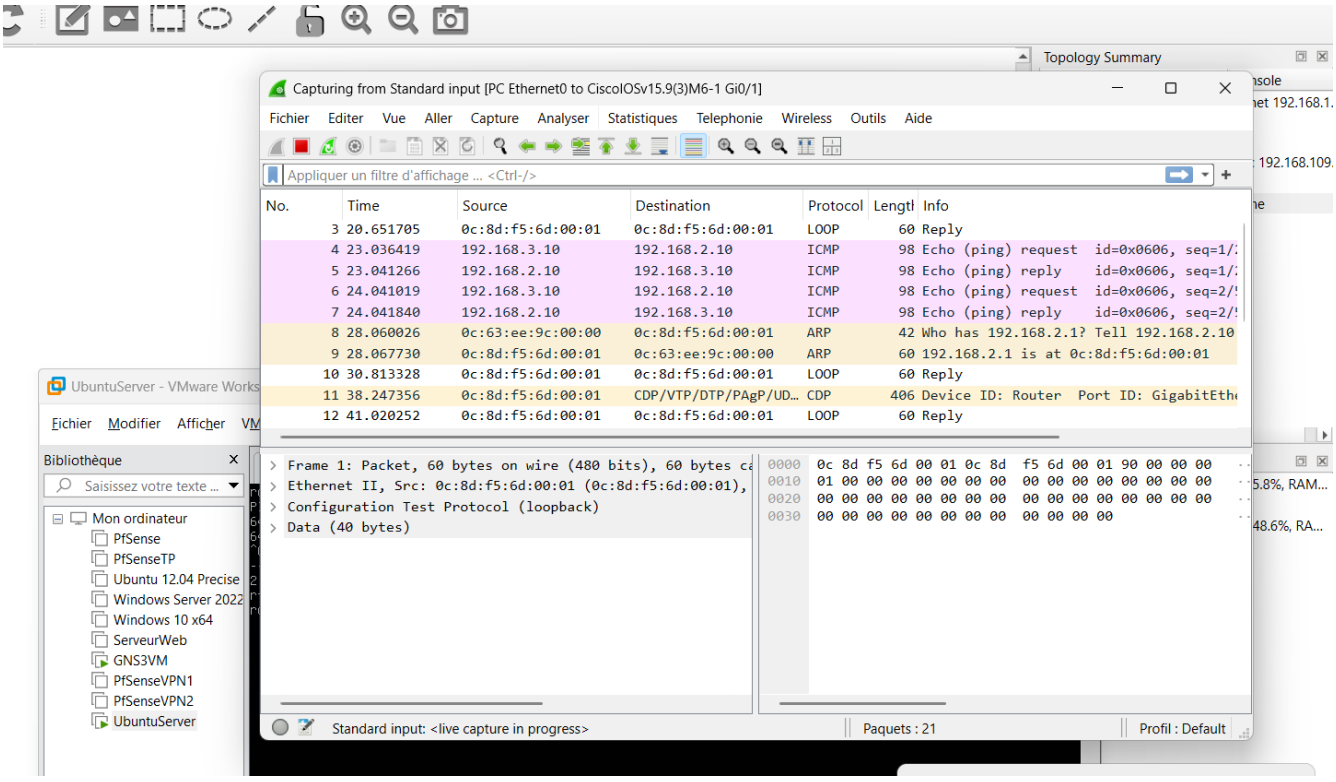
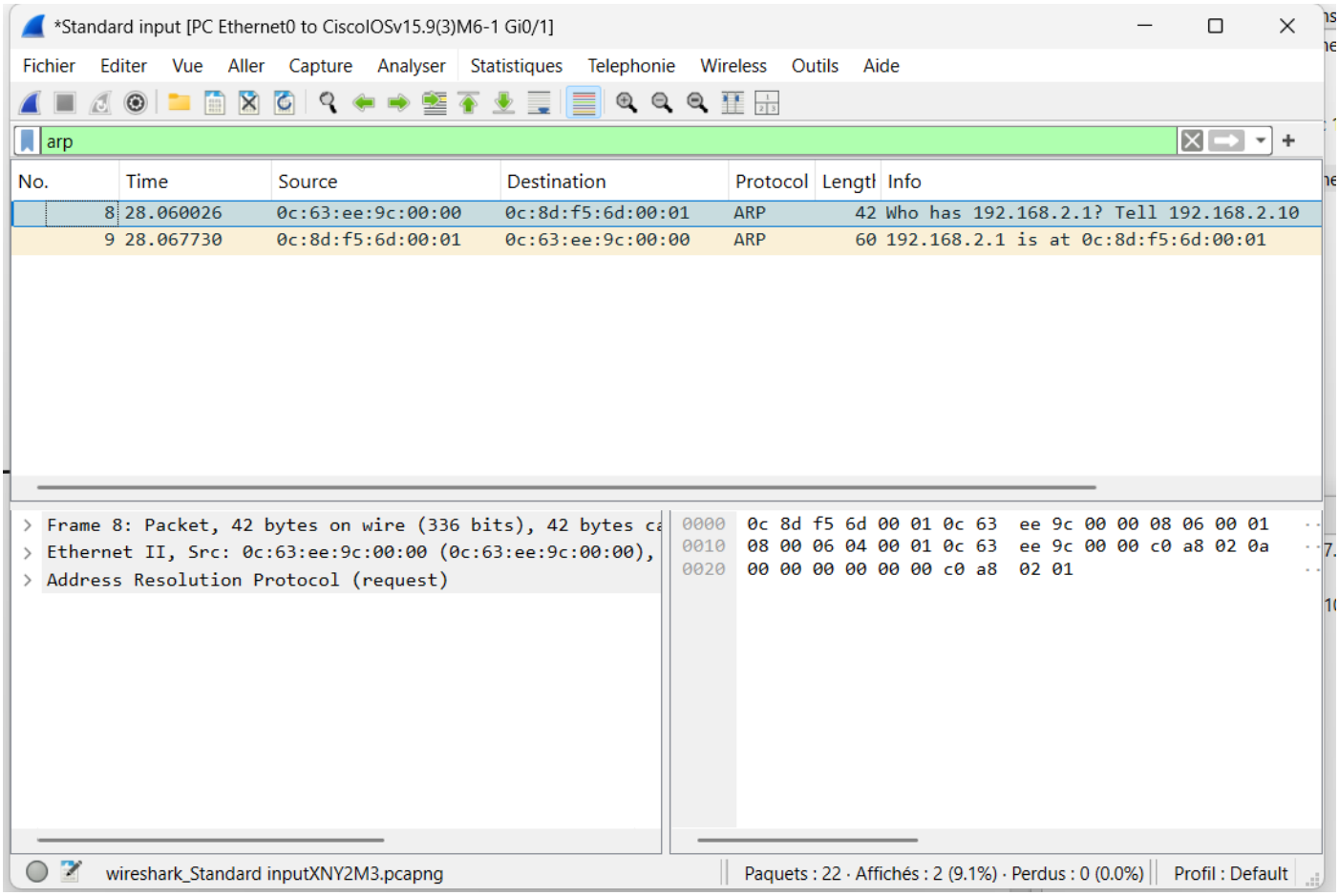
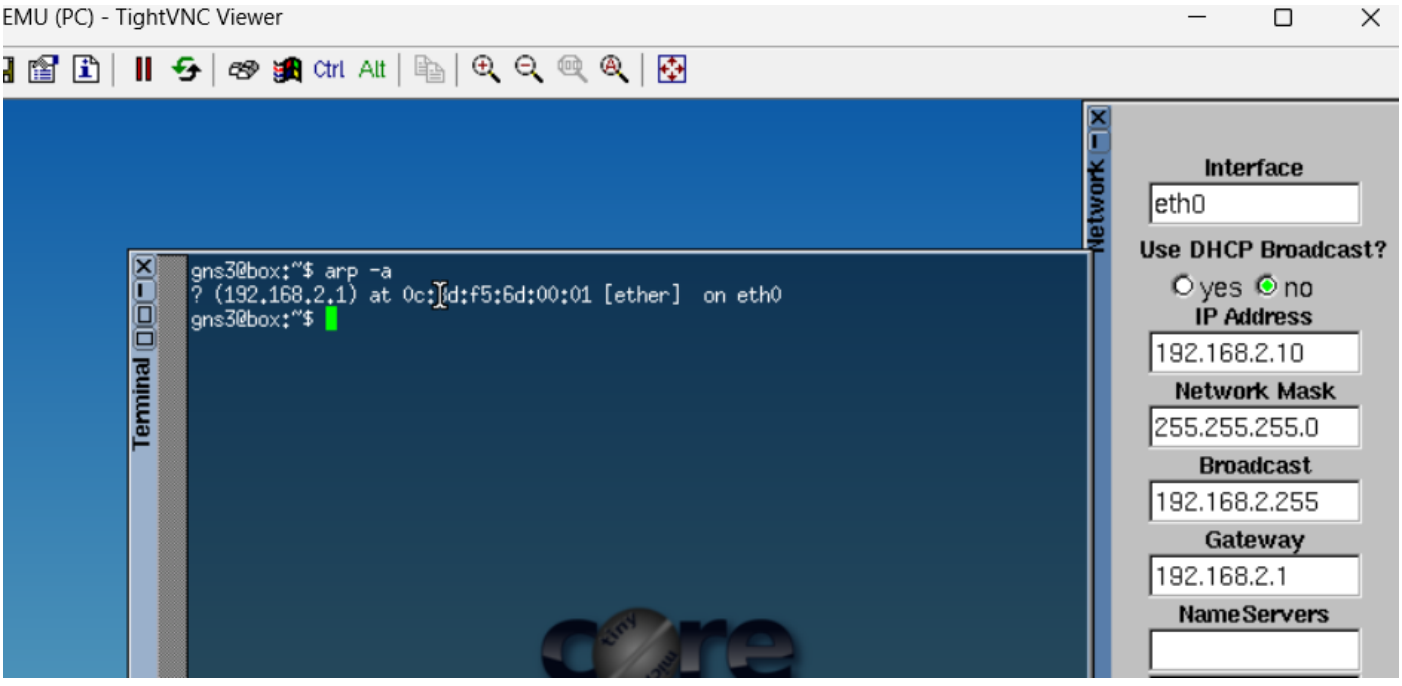


Image 9 : paquet ARP



Cette capture montre les échanges ARP permettant de faire correspondre une adresse IP à une adresse MAC. Ce mécanisme est indispensable pour la communication sur un réseau local.

Image 10 : Table Arp Coté Machine



Cette capture dans l’image 10 montre la table ARP de la machine, qui contient les correspondances entre les adresses IP et les adresses MAC connues.

Conclusion

Ce TP a permis de mettre en œuvre une architecture réseau simple et d’en valider le fonctionnement à travers différents tests de connectivité.
L’analyse des paquets avec Wireshark a permis d’identifier les échanges ICMP ainsi que les requêtes ARP nécessaires à la résolution des adresses IP en adresses MAC.
Ce travail a permis de mieux comprendre les mécanismes fondamentaux des communications réseau et le rôle des principaux protocoles.