Compte rendu de TP

Analyse du trafic réseau avec Wireshark
Et
Simulation d'un réseau local avec Packet Tracer

Etudiant : Stanley LAFLEUR

Programme : DESS - Administration de base de données
Matière : Architecture des Réseaux
Enseignante : Judith Soulamite Nouho Noutat

25 Mars 2025

Table des matières

Compte rendu du TP-1

Objectifs du TP-1

- Capturer et analyser des requêtes ICMP (ping) avec Wireshark
- Identifier les adresses IP et MAC dans les trames réseau
- Comparer le comportement des pings locaux et distants

Matériel et environnement

- 2 PCs avec Windows
    - 1 PC avec Wireshark installé (PC1)
    - 1 PC disponible pour les tests ping (PC2)
- Accès à Internet et au réseau local (LAN)
- Invite de commandes pour les tests ping

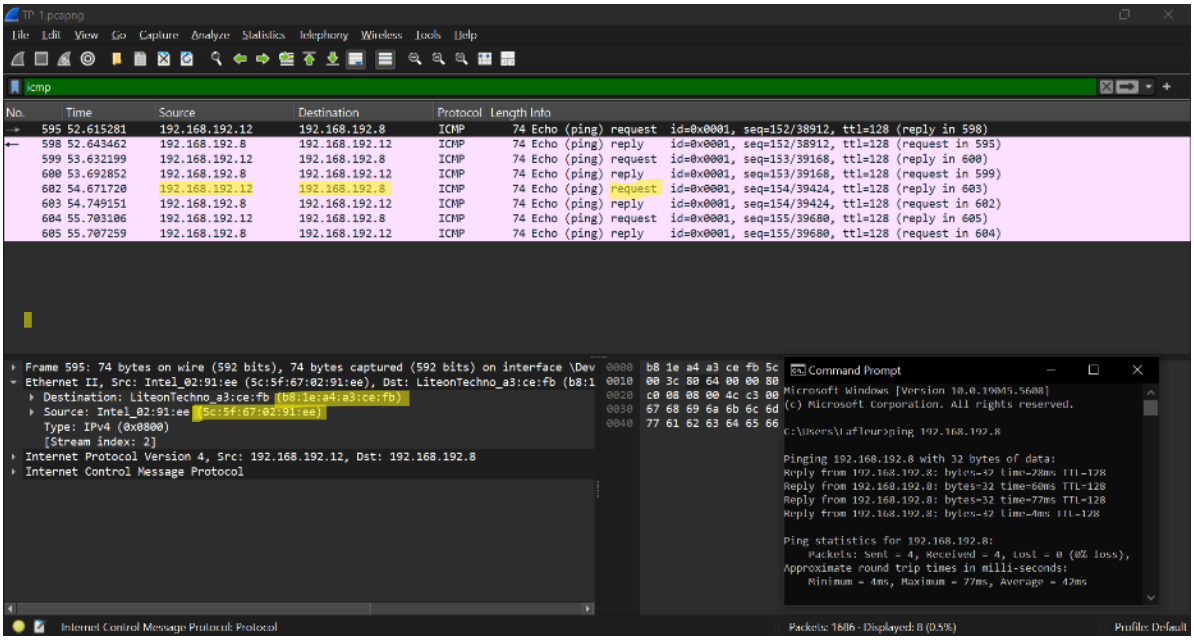
Déroulement des tests

Capturer et analyser les données ICMP locales avec Wireshark

1. Étape préliminaire : Récupération des adresses d'interface
   Avec la commande $ipconfig\ /all$ dans l'invité de commande de chaque PC on a :

	Adresse IP	Adresse MAC
PC1	192.168.192.12	5C-5F-67-02-91-EE
PC2	192.168.192.8	B8-1E-A4-A3-CE-FB

2. Lancement de Wireshark pour capturer des données avec option de filtre ICMP.
3. Dans le CMD du PC1 avec la commande $ping$ 192.168.192.8



4. **Questions**
   - L'adresse MAC de la source correspond-elle à l'interface de votre ordinateur ?
   - Oui (PC1)
   - L'adresse MAC de la destination dans Wireshark correspond-elle à l'adresse MAC du membre de votre équipe ?
   - Oui (PC2)
   - Comment votre ordinateur obtient-il l'adresse MAC de l'ordinateur de destination des requêtes ping ?

- Il utilise le protocole ARP (Address Resolution Protocol) pour demander l'adresse MAC correspondant à l'adresse IP de destination, puis stocke cette correspondance dans la table ARP.

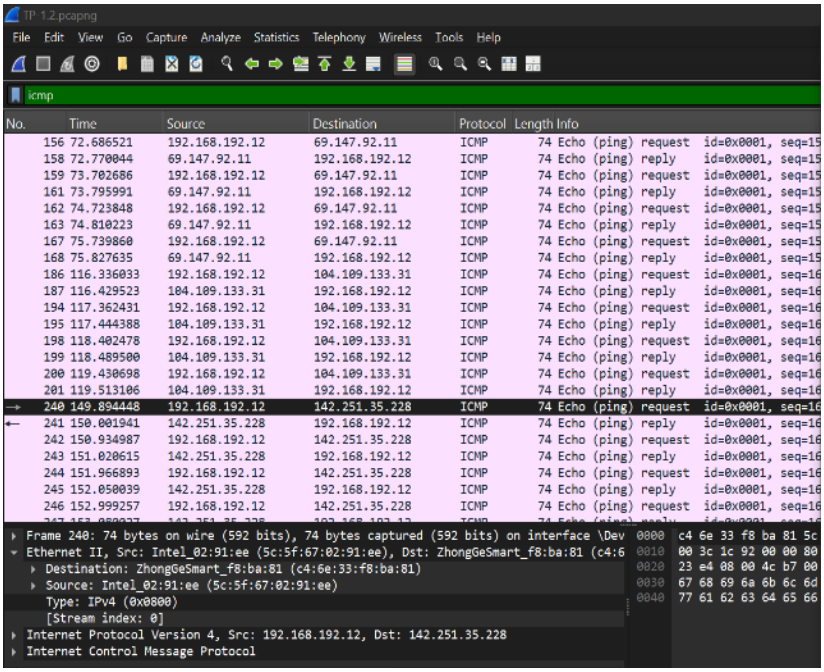
Capturer et analyser les données ICMP d'hôtes distants avec Wireshark.

1. Ping vers des hôtes distants

1) www.yahoo.com

2) www.cisco.com

3) www.google.com



2. Examen et analyse des données à partir des hôtes distants

Site pingé	Adresse IP	Adresse MAC observée
www.yahoo.com	69.147.92.11	C4:6E:33:F8:BA:81 (routeur)
www.cisco.com	69.147.92.11	C4:6E:33:F8:BA:81 (routeur)
www.google.com	69.147.92.11	C4:6E:33:F8:BA:81 (routeur)

3. **Questions**

1. Quel élément important tirez-vous de ces informations ?

R- Pour les hôtes distants, l'adresse MAC de destination est celle de l'interface réseau du routeur situé dans notre réseau local.

2. En quoi ces informations diffèrent-elles des informations de requêtes ping locales que vous avez reçues dans la deuxième partie ?

R- Pour les hôtes distants, l'adresse MAC de destination est celle de l'interface réseau du routeur situé dans notre réseau local.

3. Pourquoi Wireshark affiche-t-il l'adresse MAC réelle des hôtes locaux, mais pas l'adresse MAC réelle des hôtes distants ?

R- Wireshark affiche l'adresse MAC réelle des hôtes locaux, car l'ordinateur communique directement avec eux sur le réseau local. Pour les hôtes distants, situés en dehors du réseau local, les paquets sont envoyés au routeur, qui les transmet ensuite vers leur destination. Ainsi, l'adresse MAC visible dans Wireshark est celle du routeur, car les adresses MAC ne sont pas transmises au-delà du réseau local.

Conclusion

Ce TP a permis de comprendre la différence de traitement entre un trafic local et distant. Wireshark met en évidence les différents niveaux du modèle OSI, en particulier les couches liaison de données (MAC) et réseau (IP). On retient que les adresses MAC ne sont utilisées **que dans le réseau local**, et qu'un ping vers Internet passe toujours par le routeur, ce qui explique pourquoi on ne voit jamais l'adresse MAC réelle d'un hôte distant.

Compte rendu du TP-2

Objectifs du TP

- Comprendre le fonctionnement de Packet Tracer
- Créer un réseau local simple entre deux ordinateurs
- Configurer les adresses IP
- Tester la connectivité à l'aide de commandes réseau (ping)
- Utiliser le mode simulation pour visualiser les trames

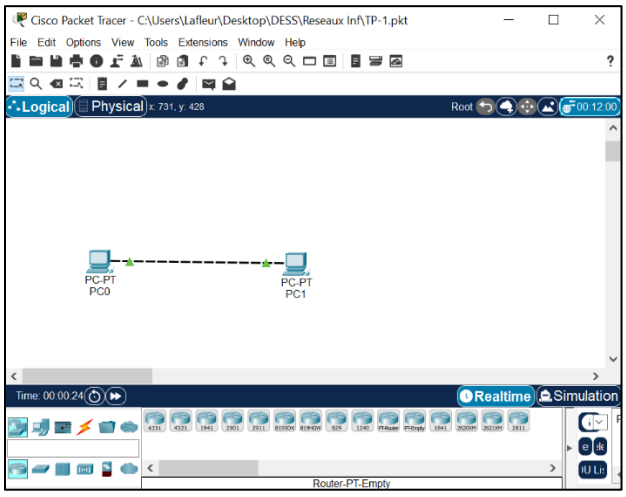
Matériel et environnement

- Ordinateur portable avec windows
- Logiciel : Cisco Packet Tracer
- Matériel virtuel utilisé : 2 PC-PT (ordinateurs), 1 câble croisé
- Connexion : FastEthernet entre les deux ordinateurs

Déroulement du TP

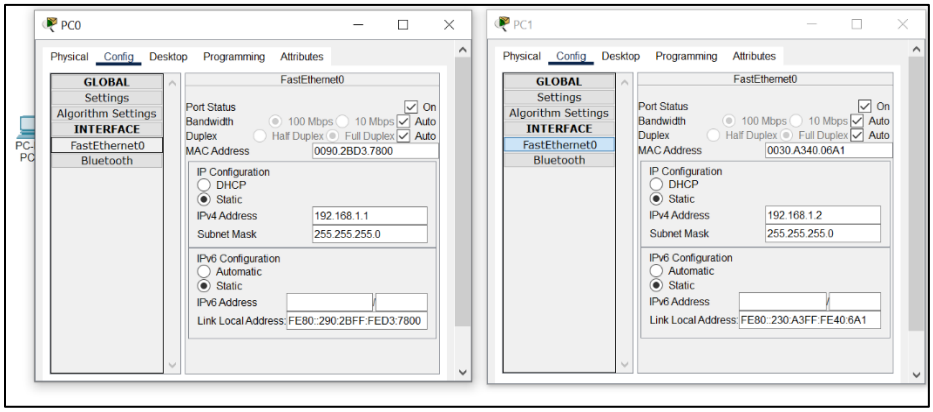
1) **Placement des équipements**

   a) Placer deux ordinateurs (PC-PT) dans la zone de travail.
   b) Choisir le type de câble (croisé) et relier les deux ordinateurs via leurs ports FastEthernet.



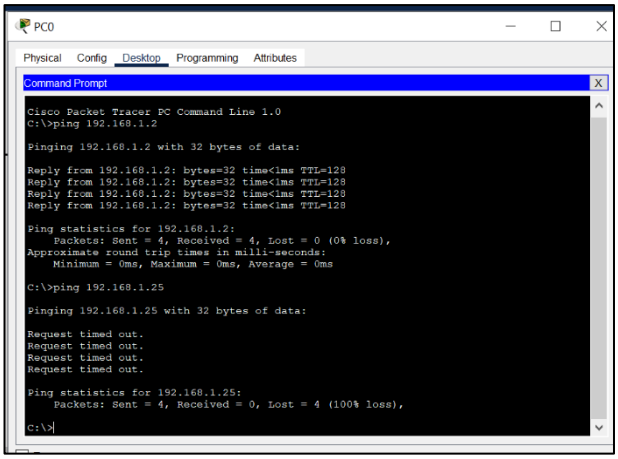
2) Configuration des adresses IP

a) PC1 : IP = 192.168.1.1 / Masque = 255.255.255.0
b) PC2 : IP = 192.168.1.2 / Masque = 255.255.255.0



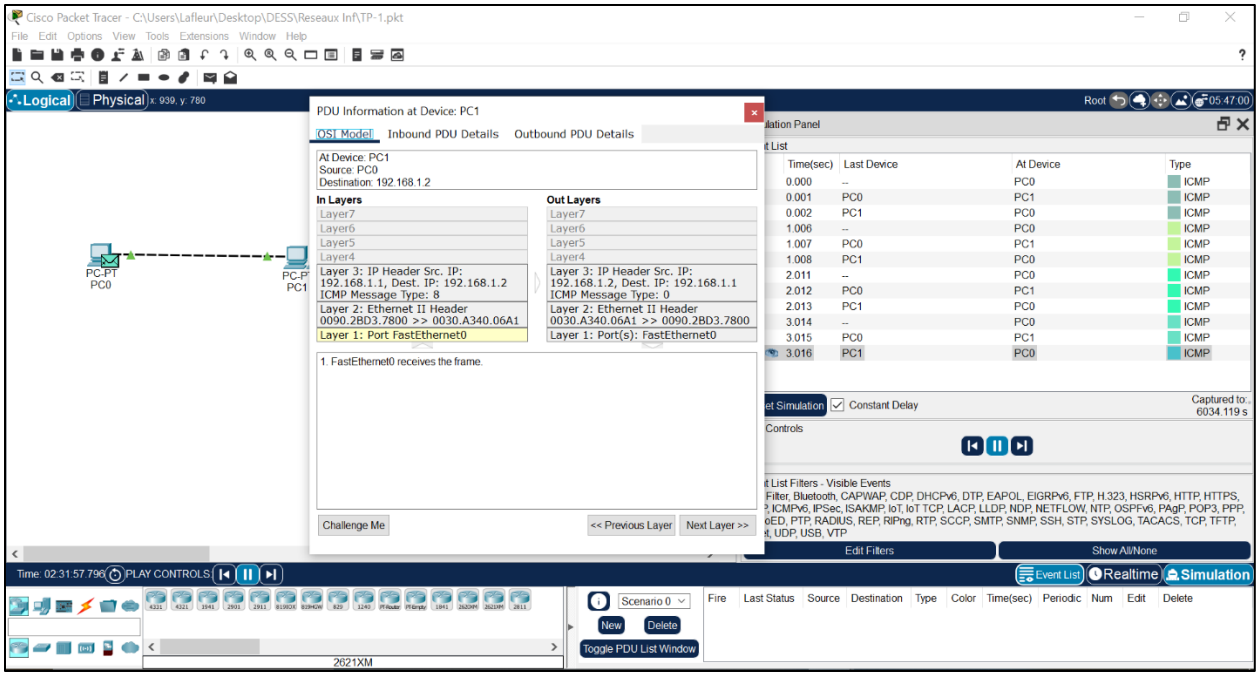
3) Test de connectivité avec la commande ping

a) Depuis PC1, envoyer un ping vers l'adresse IP de PC2
b) Résultat : les paquets sont reçus avec succès → connectivité OK
c) Ensuite, test vers une adresse IP inexistante (192.168.10.25) → aucun paquet reçu



4) Passage en mode simulation

a) Passage du mode temps réel à simulation
b) Visualisation du cheminement des trames ICMP entre les deux PC
c) Analyse de trames : possibilité de voir les couches OSI et les données contenues



Conclusion

Ce TP nous a permis de créer un réseau local simple, de configurer les adresses IP, de tester la communication entre deux machines, et d'observer le cheminement des trames via le mode simulation. Packet Tracer est un outil visuel très utile pour comprendre le fonctionnement des protocoles réseau de manière progressive et intuitive.