■ FORMATION WIRESHARK

BTS SIO SISR - Travaux Dirigés

TD1 : Les couches basses - Ethernet et IP

Couches 2 et 3 du modèle OSI

Durée estimée	45 minutes
Prérequis	Wireshark installé, droits de capture
Matériel nécessaire	PC avec connexion Internet
Livrables	Fichier .pcapng + Réponses aux questions

■ Objectifs pédagogiques

✓ Comprendre le rôle des couches 2 (Liaison) et 3 (Réseau) du modèle OSI

✓ Différencier adresse MAC et adresse IP

✓ Observer le fonctionnement du protocole ICMP (ping)

✓ Analyser une trame Ethernet dans Wireshark

✓ Comprendre pourquoi les paquets passent par le routeur local

■ Programme du TD

PARTIE 1	Rappels théoriques	5 min	■
PARTIE 2	Manipulation pratique	20 min	■
PARTIE 3	Questions d'analyse	15 min	■
PARTIE 4	Livrables à rendre	5 min	■

■ PARTIE 1 : Rappels théoriques

(À lire avant de commencer la manipulation)

Le modèle OSI - Vue d'ensemble

Le modèle OSI (Open Systems Interconnection) est un modèle de référence qui décompose les communications réseau en 7 couches distinctes. Chaque couche a un rôle spécifique et communique avec les couches adjacentes.

Couche	Nom	Protocoles / Exemples	Rôle
7	APPLICATION	HTTP, DNS, FTP	Interface utilisateur
6	PRÉSENTATION	SSL/TLS, JPEG	Format des données
5	SESSION	NetBIOS, RPC	Gestion des sessions
4	TRANSPORT	TCP, UDP	Ports, fiabilité
3	RÉSEAU	IP, ICMP, ARP	Adressage logique (IP)
2	LIAISON	Ethernet, Wi-Fi	Adressage physique (MAC)
1	PHYSIQUE	Câbles, ondes	Support physique

■ Focus du TD1 : Couches 2 et 3

Couche 2 - LIAISON (Data Link)

• **Rôle :** Communication entre équipements sur le **même réseau local**

• **Adressage :** Adresse MAC (48 bits, exemple : 00:1A:2B:3C:4D:5E)

• **Équipement principal :** Switch (commutateur)

• **Protocole :** Ethernet (câblé) ou Wi-Fi (sans fil)

Couche 3 - RÉSEAU (Network)

• **Rôle :** Routage entre **différents réseaux**

• **Adressage :** Adresse IP (IPv4 : 32 bits, exemple : 192.168.1.10)

• **Équipement principal :** Routeur

• **Protocoles :** IP, ICMP, ARP

■ **Point clé à retenir :** La couche 2 (MAC) fonctionne uniquement sur le réseau local, tandis que la couche 3 (IP) permet de communiquer entre réseaux différents via des routeurs.

■ PARTIE 2 : Manipulation pratique

Objectif de l'exercice

Capturer le trafic généré par une commande **ping** pour analyser les couches 2 et 3 du modèle OSI. Le ping utilise le protocole ICMP (Internet Control Message Protocol) qui permet de tester la connectivité réseau.

■ Étapes de la manipulation

Étape 1 : Préparer Wireshark

• Ouvre Wireshark
• Choisis ton interface Wi-Fi (exemple : wlp0s20f3)
• **NE LANCE PAS ENCORE** la capture

Étape 2 : Lancer la capture

• Clique sur le bouton bleu (aileron de requin) ■
• La capture démarre immédiatement

Étape 3 : Générer du trafic

• Ouvre un terminal
• Tape la commande : `ping -c 4 8.8.8.8`
• Cette commande envoie 4 paquets ICMP vers le DNS de Google

Étape 4 : Arrêter la capture

• Attends que le ping se termine (quelques secondes)
• Clique sur le carré rouge ■ dans Wireshark

Étape 5 : Filtrer les paquets

• Dans la barre de filtre de Wireshark (en haut)
• Tape : `icmp`
• Appuie sur Entrée
• Tu ne verras plus que les paquets ICMP

Étape 6 : Sauvegarder

• File → Save As
• Nomme le fichier : `TD1_ping.pcapng`
• Enregistre-le dans un dossier que tu retrouveras facilement

> ■ **Conseil :** Si tu vois trop de paquets dans ta capture (plus de 50), c'est normal ! Le filtre ICMP permet d'isoler uniquement les 8 paquets qui nous intéressent (4 requêtes + 4 réponses).

■ PARTIE 3 : Questions d'analyse

> ■■ **IMPORTANT :** Ne cherche PAS les réponses sur Internet ! Toutes les réponses se trouvent dans ta capture Wireshark. Observe attentivement les détails de chaque paquet.

■ Questions sur la Couche 2 (Liaison)

Sélectionne le **premier paquet** dans ta capture (celui avec 'Echo request').

Q1. Dans le panneau du milieu, déroule la section **« Ethernet II »**. Quelles sont les **deux adresses MAC** que tu vois ? (Cherche 'Source' et 'Destination')

Q2. L'adresse MAC source, c'est celle de quel équipement ?
A) Ton ordinateur
B) Ton routeur/box
C) Le serveur 8.8.8.8

Q3. L'adresse MAC de destination, c'est celle de quel équipement ?
A) Ton ordinateur
B) Ton routeur/box
C) Le serveur 8.8.8.8

Q4. Pourquoi l'adresse MAC de destination n'est PAS celle du serveur Google (8.8.8.8) ?
Réfléchis au rôle de la couche 2...

■ Questions sur la Couche 3 (Réseau)

Toujours sur le même paquet, déroule la section **« Internet Protocol Version 4 »**.

Q5. Quelle est l'adresse IP **source** ? C'est l'adresse de qui ?

Q6. Quelle est l'adresse IP **de destination** ? (C'est bien 8.8.8.8 normalement !)

Q7. Compare avec les adresses MAC (Q1). Est-ce que les adresses IP et MAC correspondent de la même manière ?
• IP source → MAC source ?
• IP destination → MAC destination ?

Q8. Regarde le champ **« Time to Live » (TTL)**. Quelle est sa valeur ? (Un nombre comme 64, 128...)

Q9. À quoi sert le TTL ? *Indice : 'Time to Live' = durée de vie... de quoi ?*

■ Questions sur le protocole ICMP

Déroule la section **« Internet Control Message Protocol »**.

Q10. Quel est le **type** du message ICMP ?
Indice : Type 8 = Echo Request (demande) / Type 0 = Echo Reply (réponse)

Q11. Sélectionne maintenant **le paquet de réponse** (celui qui vient de 8.8.8.8). Quel est son type ICMP ?

Q12. Compare les adresses MAC et IP du paquet de **réponse** avec celles du paquet **envoyé**. Qu'est-ce qui a changé ?

■ Question de synthèse (difficile mais importante !)

Q13. Tu as envoyé un ping vers **8.8.8.8** (serveur Google aux États-Unis probablement), mais l'adresse MAC de destination est celle de **ta box/routeur**. Explique pourquoi c'est normal et comment le paquet arrive quand même jusqu'à Google.

Indice : Pense aux rôles différents des couches 2 et 3 !

■ PARTIE 4 : Livrables à rendre

Tu dois me renvoyer les éléments suivants :

■ Ton fichier de capture : `TD1_ping.pcapng`

■ Tes réponses aux 13 questions (numérotées de Q1 à Q13)

■ Une ou deux captures d'écran de Wireshark montrant :
• La section Ethernet II déroulée
• La section IPv4 déroulée

■ Conseils pour réussir

• Prends ton temps pour observer chaque champ dans Wireshark

• Double-clique sur un paquet pour voir tous les détails

• Les réponses sont TOUTES dans ta capture, pas besoin d'Internet

• Si tu bloques, regarde bien les noms des champs dans Wireshark, ils sont explicites

• N'hésite pas à demander des clarifications si une question n'est pas claire

■■ Timing conseillé

Manipulation (capture)	15 minutes
Analyse et réponses aux questions	25 minutes
Pause si besoin	5 minutes

■ Critères d'évaluation

Je vérifierai que tu as compris :

✓ La différence entre adresse MAC et adresse IP
✓ Le rôle de chaque couche (2 et 3)
✓ Pourquoi on utilise l'adresse MAC du routeur même si on communique avec une IP distante
✓ Le fonctionnement du protocole ICMP (ping)
✓ La notion de portée (scope) : réseau local vs. réseau distant

■ C'est parti !

Lance ta capture et réponds aux questions. Prends ton temps et observe bien chaque détail. N'hésite pas à me demander si une question n'est pas claire (mais je ne te donnerai pas la réponse directement ■).

Quand tu as fini, envoie-moi tout et on corrigera ensemble !

Bon courage ! ■