TP : Analyse de trames réseau

Objectif

Analyser une trame réseau **manuellement**, puis vérifier les résultats avec le script Python.

Matériel

- Feuille + stylo
- Ordinateur avec Python 3
- Trames fournies (`trame.txt`)

Déroulement

Étape 1 – Analyse papier

1. Lecture des octets
2. Décodage Ethernet
3. Décodage IPv4 ou ARP
4. Décodage ICMP ou TCP si nécessaire
5. Remplissage du tableau d'analyse

Étape 2 – Vérification

```
python analyse_trame.py trame.txt
```

- Comparaison champ par champ
- Correction des erreurs éventuelles

Méthodologie

- Toujours **commencer sur papier**
- Travailler **octet par octet**
- Respecter les tailles d'en-têtes :
  - Ethernet : 14
  - IPv4 : ≥ 20
  - TCP : ≥ 20
  - ICMP : 4
  - ARP : 28 octets
- Utiliser systématiquement les **tableaux d'analyse**

Trames fournies

1. Trame A

```
ff ff ff ff ff ff
00 11 22 33 44 55
08 00
45 00 00 34 1c 46 40 00 40 06 a6 ec
c0 a8 01 01
c0 a8 01 02
00 50 01 bb 00 00 00 01 00 00 00 00 50 02 71 10 00 00 00 00
```

Champ	Valeur à compléter
MAC destination	
MAC source	
Type Ethernet	
IPv4 Version	
IHL (en-tête IPv4)	
Longueur totale	
TTL	
Protocole IPv4	
IP source	
IP destination	
Port source TCP	
Port destination TCP	
Numéro de séquence	
Numéro d'acknowledgment	
Flags TCP	

2. Trame B

```
ff ff ff ff ff ff
00 11 22 33 44 55
08 00
45 00 00 1c 1c 46 40 00 40 01 a6 f5
c0 a8 01 01
c0 a8 01 02
08 00 f7 ff 00 01 00 01
```

Champ	Valeur à compléter
MAC destination	
MAC source	
Type Ethernet	
IPv4 Version	
IHL (en-tête IPv4)	
Longueur totale	
TTL	
Protocole IPv4	
IP source	
IP destination	
Type ICMP	
Code ICMP	
Checksum ICMP	

3. Trame C

```
ff ff ff ff ff ff
00 11 22 33 44 55
08 06
00 01 08 00 06 04 00 01
00 11 22 33 44 55
c0 a8 01 01
00 00 00 00 00 00
c0 a8 01 02
```

Champ	Valeur à compléter
MAC destination	
MAC source	
Type Ethernet	
Opcode ARP	
MAC source ARP	
IP source ARP	
MAC destination ARP	
IP destination ARP	

4. Trame D

```
aa bb cc dd ee ff
11 22 33 44 55 66
08 00
45 00 00 28 12 34 40 00 40 06 00 00
0a 00 00 01
0a 00 00 02
d4 31 00 50 12 34 56 78 00 00 00 00 50 18 20 00 00 00 00 00
```

Champ	Valeur à compléter
MAC destination	
MAC source	
Type Ethernet	
IPv4 Version	
IHL (en-tête IPv4)	
Longueur totale	
TTL	
Protocole IPv4	
IP source	
IP destination	
Port source TCP	
Port destination TCP	
Numéro de séquence	
Numéro d'acknowledgment	
Flags TCP	

5. Trame E

```
00 11 22 33 44 55
ff ff ff ff ff ff
08 00
45 00 00 1c 1c 46 40 00 40 01 a6 f6
c0 a8 01 02
c0 a8 01 01
00 00 f7 ff 00 01 00 01
```

Champ	Valeur à compléter
MAC destination	
MAC source	
Type Ethernet	
IPv4 Version	
IHL (en-tête IPv4)	
Longueur totale	
TTL	
Protocole IPv4	
IP source	
IP destination	
Type ICMP	
Code ICMP	
Checksum ICMP	

6. Trame F

```
00 11 22 33 44 55
ff ff ff ff ff ff
08 06
00 01 08 00 06 04 00 02
00 11 22 33 44 55
c0 a8 01 01
00 aa bb cc dd ee
c0 a8 01 01
```

Champ	Valeur à compléter
MAC destination	
MAC source	
Type Ethernet	
Opcode ARP	
MAC source ARP	
IP source ARP	
MAC destination ARP	
IP destination ARP	