

Fiche de référence : formats de trames réseau

Ethernet (IEEE 802.3)

Champ	Taille	Description
MAC destination	6 octets	Adresse MAC du destinataire
MAC source	6 octets	Adresse MAC de l'émetteur
Type / Longueur	2 octets	Type de protocole encapsulé (0x0800 = IPv4, 0x0806 = ARP)

Remarques :

- Les adresses MAC sont en hexadécimal (ex : **00:11:22:33:44:55**).
 - Ethernet minimum = 14 octets d'en-tête.
-

IPv4 (RFC 791)

Champ	Taille	Description
Version	4 bits	Version IP (4 pour IPv4)
IHL (Header Length)	4 bits	Longueur de l'en-tête en multiples de 4 octets
Type of Service (TOS)	1 octet	Priorité et QoS
Longueur totale	2 octets	Taille totale de la trame IP (en-tête + données)
Identification	2 octets	Numéro pour fragmenter/réassembler
Flags + Fragment	2 octets	Fragmentation (MF, DF, offset)
TTL	1 octet	Time To Live (limite de sauts)
Protocole	1 octet	TCP=6, ICMP=1, UDP=17
Checksum	2 octets	Contrôle d'erreur de l'en-tête
IP source	4 octets	Adresse IPv4 source
IP destination	4 octets	Adresse IPv4 destination

Remarques :

- IHL minimum = 5 → en-tête de 20 octets.
 - Les adresses IP sont en décimal pointé (**192.168.1.1**).
 - RFC 791 : <https://www.rfc-editor.org/rfc/rfc791>
-

ARP (RFC 826)

Champ	Taille	Description
Hardware type	2 octets	Ethernet = 1
Protocol type	2 octets	IPv4 = 0x0800
Hardware size	1 octet	Taille adresse MAC (6)
Protocol size	1 octet	Taille adresse IP (4)
Opcode	2 octets	1 = requête, 2 = réponse
MAC source	6 octets	Adresse MAC de l'émetteur
IP source	4 octets	Adresse IP de l'émetteur
MAC destination	6 octets	Adresse MAC du destinataire
IP destination	4 octets	Adresse IP du destinataire

Remarque : ARP sert à résoudre l'adresse IP → MAC. RFC 826 : <https://www.rfc-editor.org/rfc/rfc826>

TCP (RFC 793)

Champ	Taille	Description
Port source	2 octets	Port du processus émetteur
Port destination	2 octets	Port du processus destinataire
Numéro de séquence	4 octets	Ordre des octets envoyés
Numéro d'ack	4 octets	Numéro attendu suivant
Data offset	4 bits	Taille de l'en-tête TCP
Flags	1 octet	URG, ACK, PSH, RST, SYN, FIN
Window	2 octets	Taille fenêtre de réception
Checksum	2 octets	Contrôle d'erreur
Urgent pointer	2 octets	Si flag URG = 1

ICMP (RFC 792)

Champ	Taille	Description
Type	1 octet	Type de message (ex : 8 = Echo Request, 0 = Echo Reply)
Code	1 octet	Sous-type / précision
Checksum	2 octets	Contrôle d'erreur

Fiche aide-mémoire : Trames réseau Ethernet → IPv4 → TCP/ICMP/ARP

Encapsulation simplifiée

```
[ Ethernet ] → [ IPv4 ] → [ TCP / ICMP ]  
ou  
[ Ethernet ] → [ ARP ]
```

- Chaque bloc = un **en-tête** avec champs spécifiques.
 - Les **données utiles** suivent toujours le dernier en-tête.
 - Travailler **octet par octet** est la clé pour l'analyse manuelle.
-

Ethernet (14 octets)

```
| MAC dest (6) | MAC src (6) | Type (2) |
```

- MAC : hexadécimal (**00:11:22:33:44:55**)
 - Type : 0x0800 = IPv4, 0x0806 = ARP
-

IPv4 (20 octets minimum)

```
| Ver+IHL (1) | TOS (1) | Long. totale (2) | ID (2) |  
| Flags+Frag (2) | TTL (1) | Protocole (1) | Checksum (2) |  
| IP src (4) | IP dst (4) |
```

- Version = 4
 - IHL = longueur en octets de l'en-tête (IHL×4)
 - Protocole : 1 = ICMP, 6 = TCP
 - IP : décimal pointé (**192.168.1.1**)
-

ARP (28 octets)

```
| HTYPE (2) | PTYPE (2) | HLEN (1) | PLEN (1) | Opcode (2) |  
| MAC src (6) | IP src (4) | MAC dst (6) | IP dst (4) |
```

- Opcode : 1 = requête, 2 = réponse
- Permet de trouver l'adresse MAC d'une IP

TCP (20 octets minimum)

```
| Port src (2) | Port dst (2) | Seq (4) | Ack (4) |
| Data offset (4b) | Flags (1) | Window (2) | Checksum (2) | Urgent ptr
(2) |
```

- Flags : URG, ACK, PSH, RST, SYN, FIN
- Data offset = taille en octets de l'en-tête

ICMP (4 octets + données)

```
| Type (1) | Code (1) | Checksum (2) |
```

- Type 8 = Echo Request, Type 0 = Echo Reply

Schéma de synthèse

Trame Ethernet (14)

```
+-----+
| MAC dest | MAC src | Type Ethernet |
+-----+
```

Si Type = 0x0800 (IPv4)

```
+-----+
| Ver/IHL | TOS | Long tot | ID | Flags/Frag | TTL |
| Protocole | Checksum | IP src | IP dst |
+-----+
```

→ TCP (Si protocole=6)

```
+-----+
| Port src | Port dst | Seq Num |
| Ack Num | Offset/Flags | Win |
| Checksum | Urgent Ptr |
+-----+
```

→ ICMP (Si protocole=1)

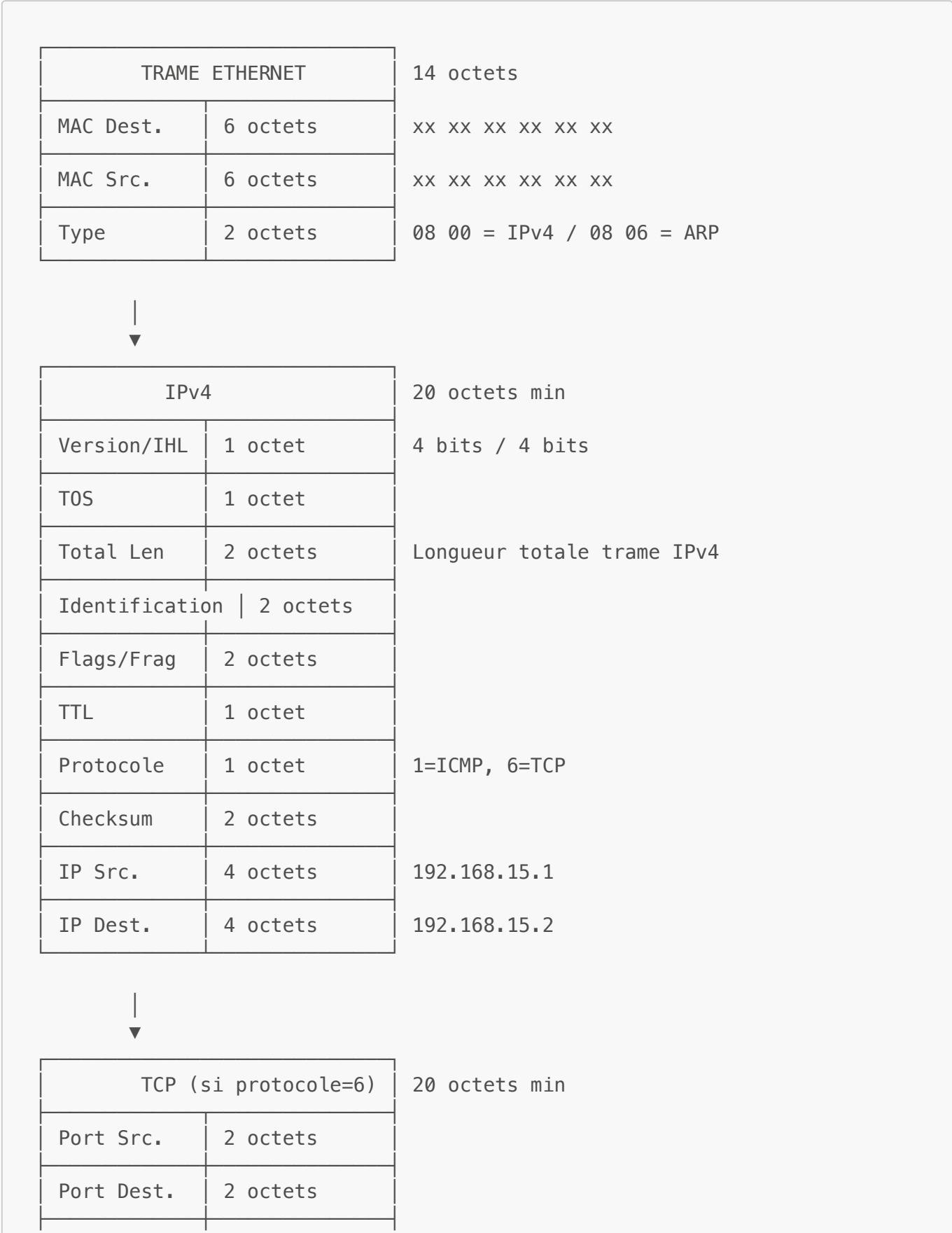
```
+-----+
| Type | Code | Cks |
+-----+
```

Si Type = 0x0806 (ARP)

```
+-----+
| HTYPE | PTYPE | HLEN | PLEN | Opcode |
+-----+
```



Schéma unifié des trames réseau



Seq Num.	4 octets	4 bits SYN, ACK, FIN...
Ack Num.	4 octets	
Data Offset	4 bits + Flags	
Flags	1 octet	
Window	2 octets	
Checksum	2 octets	
Urgent Ptr	2 octets	



ICMP (si protocole=1)		4 octets min
Type	1 octet	
Code	1 octet	
Checksum	2 octets	



ARP (Type=08 06)		28 octets 1=requête, 2=réponse
Hardware Type	2 octets	
Protocol Type	2 octets	
HLen / PLen	1+1 octet	
Opcode	2 octets	
MAC Src	6 octets	
IP Src	4 octets	
MAC Dest	6 octets	
IP Dest	4 octets	