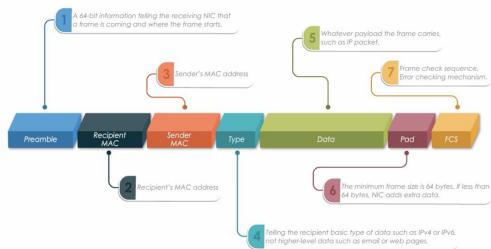


CARNUS

Enseignement
supérieur **RODEZ**



Trame Ethernet

Cours et exercices

Prof : KAMAL BOUDJELABA

6 janvier 2026

B
T
S

C
I
E
L

Table des matières

1	Format de la trame Ethernet (IEEE 802.3 et Ethernet II)	1
1.1	EtherType : Numéros de protocole	3
1.2	Exemple de protocole IEEE 802.1Q (VLAN)	4
2	Tableau récapitulatif – blocs d'une trame Ethernet II	5
3	Exercices	6
3.1	Exercice 1	6
3.2	Exercice 2	6
3.3	Exercice 3	7
3.4	Exercice 4	8
3.5	Exercice 5	8
A	Annexes	10
A.1	Trame IPV4	10
A.2	Trame IPV6	11
A.3	Trame UDP	11
A.4	Trame TCP	11
A.5	Trame ARP/RARP	12
A.6	Trame ICMP	12
A.7	Trame ICMPv6	13
A.8	Charge utile Ethernet	13

Liste des figures

1	Trame Ethernet	1
2	Trame Ethernet V2	2
3	Trame Ethernet II	3

Liste des tableaux

1	EtherType	4
2	Structure d'une trame Ethernet II	5

1. Format de la trame Ethernet (IEEE 802.3 et Ethernet II)

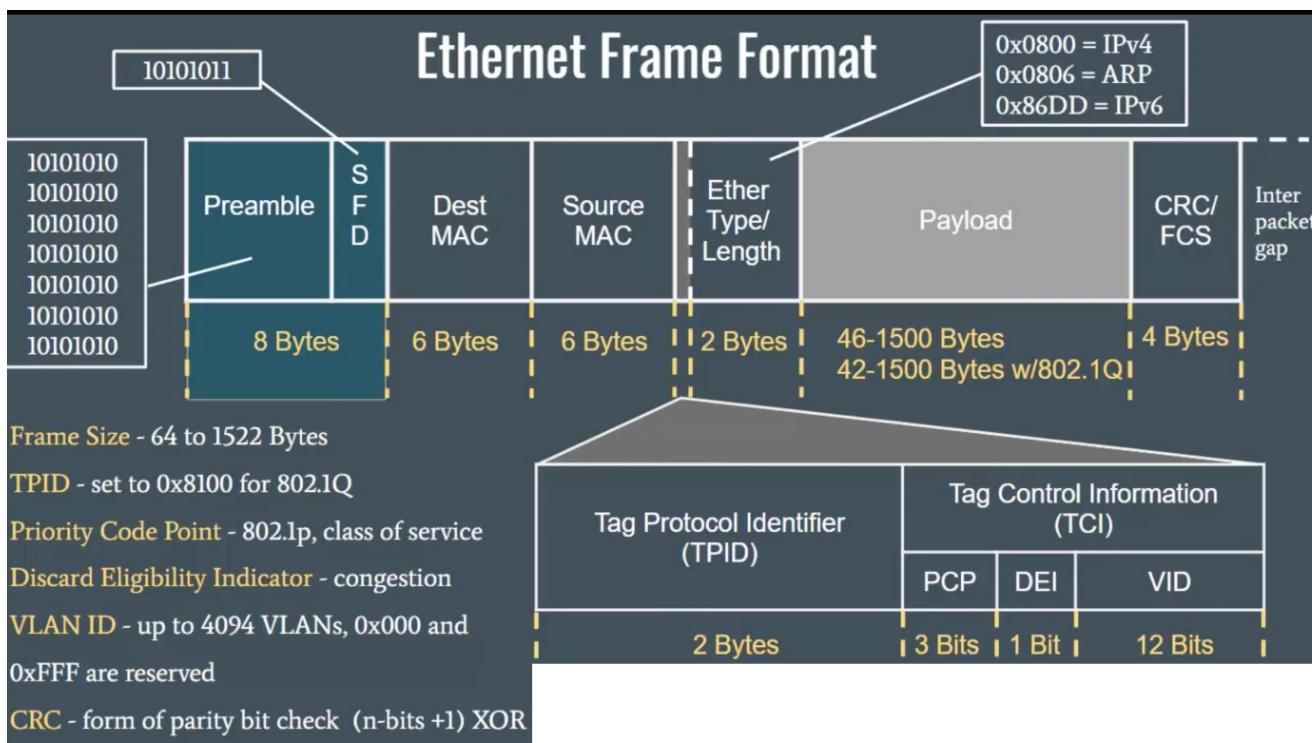
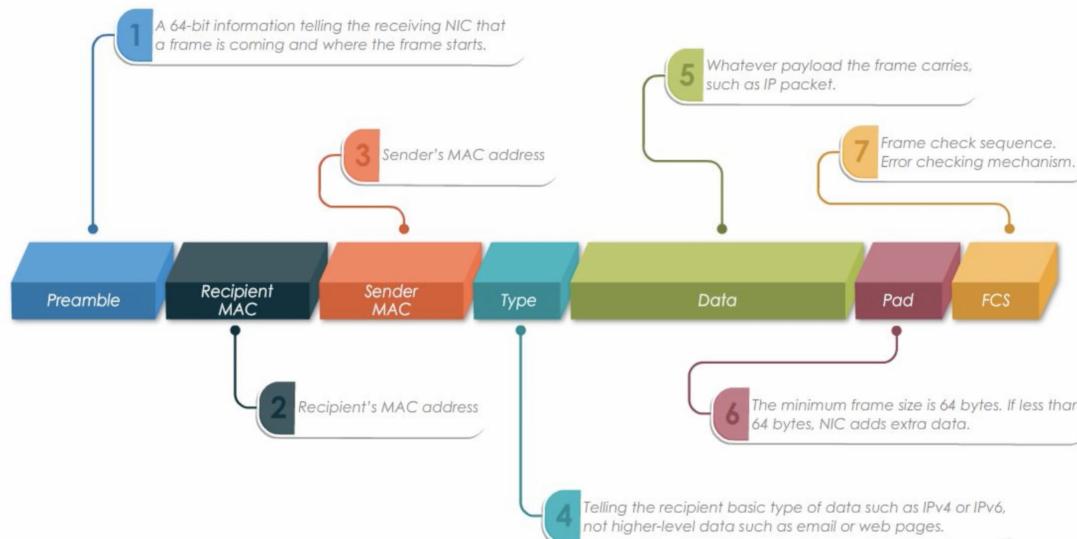
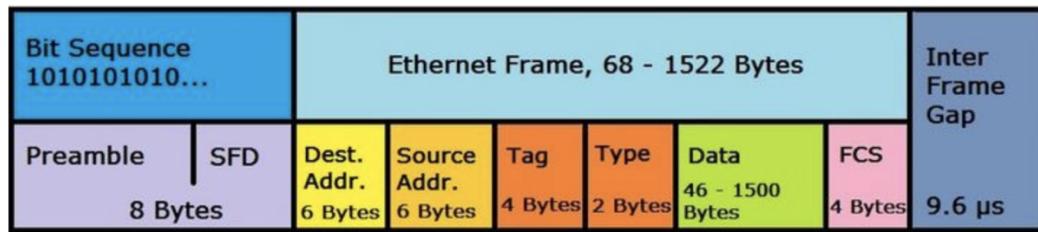


Figure 1. Trame Ethernet

Note :

Il existe principalement deux formats de trame Ethernet :

- IEEE 802.3 : champ Length + en-tête LLC (802.2)
- Ethernet II (DIX) : champ EtherType

En pratique, Ethernet II est aujourd’hui le format le plus utilisé.

Une trame Ethernet est l’unité de transmission utilisée sur les réseaux Ethernet. Elle transporte une charge utile correspondant généralement à un protocole de couche réseau (IPv4, IPv6, ARP, etc.), lequel peut encapsuler des protocoles de couche transport comme TCP ou UDP.

La norme IEEE 802.3 définit la structure des trames Ethernet transmises sur le support physique (couche 1). L’analyse de la structure d’une trame telle qu’elle est transmise sur le câble permet de comprendre l’impact temporel et les différents champs nécessaires à l’acheminement des données.

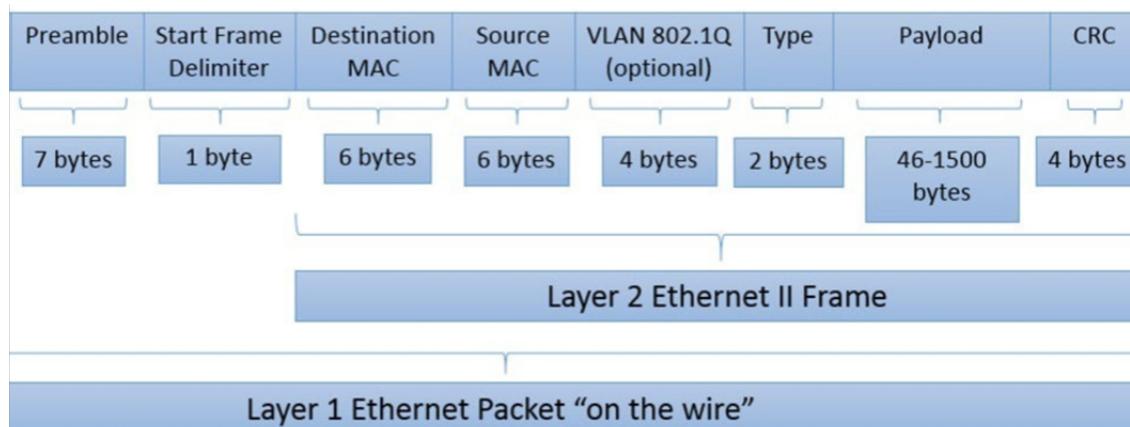


Figure 2. Trame Ethernet V2

Champs généraux d’une trame Ethernet

- Preamble : Préambule
- SFD : Start Frame Delimiter (délimiteur de début de trame)
- Destination Address : Adresse MAC de destination
- Source Address : Adresse MAC source
- Length / Type : Champ longueur (IEEE 802.3) ou type (Ethernet II)
- TPID : Tag Protocol Identifier (VLAN)
- TCI : Tag Control Information
- PCP : Priority Code Point
- DEI : Drop Eligibility Indicator
- VID : VLAN Identifier
- Data : Données (payload)
- FCS : Frame Check Sequence (CRC 32 bits)
- IPG : Inter Packet Gap (intervalle inter-trames)

Description des champs

Preamble – La trame Ethernet commence par un préambule de 7 octets constitué d’une alternance de bits 0 et 1. Il permet au récepteur de se synchroniser sur le flux binaire avant l’arrivée de la trame proprement dite.

Start Frame Delimiter (SFD) – Champ de 1 octet ayant toujours la valeur binaire 10101011. Il indique la fin du préambule et le début effectif de la trame Ethernet (adresse MAC de destination).

Destination Address – Champ de 6 octets contenant l’adresse MAC du destinataire. Cette adresse peut être unicast, multicast ou broadcast.

Source Address – Champ de 6 octets contenant l'adresse MAC de l'émetteur. Le bit de poids faible du premier octet est toujours à 0 (adresse individuelle).

Length / Type – Champ de 2 octets :

- Valeur **1500** : longueur du champ Data (format IEEE 802.3)
- Valeur **1536 (0x0600)** : identifiant du protocole encapsulé (Ethernet II)

Data – Contient les données utiles. La taille minimale est de 46 octets. Si nécessaire, des octets de bourrage (padding) sont ajoutés pour atteindre cette taille minimale. La taille maximale est de 1500 octets (hors VLAN).

Frame Check Sequence (FCS) – Champ de 4 octets contenant un CRC-32 calculé sur les champs de la trame (adresse MAC destination jusqu'aux données). Il permet de détecter les erreurs de transmission.

Remarque 1.1 :

La taille minimale d'une trame Ethernet est de 64 octets et la taille maximale est de 1518 octets. Avec l'ajout d'un tag VLAN (IEEE 802.1Q), la taille maximale passe à 1522 octets.

Trame Ethernet II (format le plus courant)

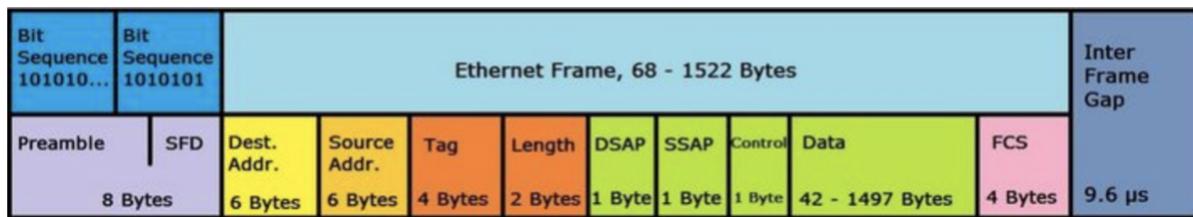


Figure 3. Trame Ethernet II

Structure Ethernet II

- Destination MAC Address : 6 octets
- Source MAC Address : 6 octets
- EtherType : 2 octets
- Data : 46 à 1500 octets
- FCS : 4 octets

Le champ EtherType indique le protocole de couche réseau encapsulé dans la trame (IPv4, IPv6, ARP, etc.). Contrairement au format IEEE 802.3, aucun champ longueur ni en-tête LLC n'est présent.

1.1 EtherType : Numéros de protocole

Indique le protocole encapsulé dans la trame Ethernet II.

EtherType	Protocol
0x0800	Internet Protocol version 4 (IPv4)
0x0806	Address Resolution Protocol (ARP)
0x8035	Reverse Address Resolution Protocol (RARP)
0x8100	VLAN-tagged frame (IEEE 802.1Q)
0x86DD	Internet Protocol Version 6 (IPv6)
0x8808	Ethernet flow control
0x8809	Link Aggregation Control Protocol
0x8847	MPLS unicast
0x8848	MPLS multicast
0x8863	PPPoE Discovery Stage
0x8864	PPPoE Session Stage
0x88E	EAP over LAN (IEEE 802.1X)
0x889A	HyperSCSI (SCSI over Ethernet)
0x88A2	ATA over Ethernet
0x88CC	Link Layer Discovery Protocol (LLDP)
0x88E5	MAC security (IEEE 802.1AE)
0x8906	Fibre Channel over Ethernet (FCoE)
0x8914	FoE Initialization Protocol
0x9100	VLAN-tagged (IEEE 802.1Q) frame with double tagging

Table 1. EtherType

1.2 Exemple de protocole IEEE 802.1Q (VLAN)

- a – PCP (Priority Code Point) : champ sur 3 bits indiquant la priorité de la trame (8 niveaux).
- b – DEI (Drop Eligibility Indicator) : champ sur 1 bit indiquant si la trame peut être éliminée en cas de congestion.
- c – VLAN ID : champ sur 12 bits identifiant le VLAN (valeurs de 1 à 4094). La valeur 0 indique l'absence de VLAN mais permet l'utilisation de la priorité.

2. Tableau récapitulatif – blocs d'une trame Ethernet II

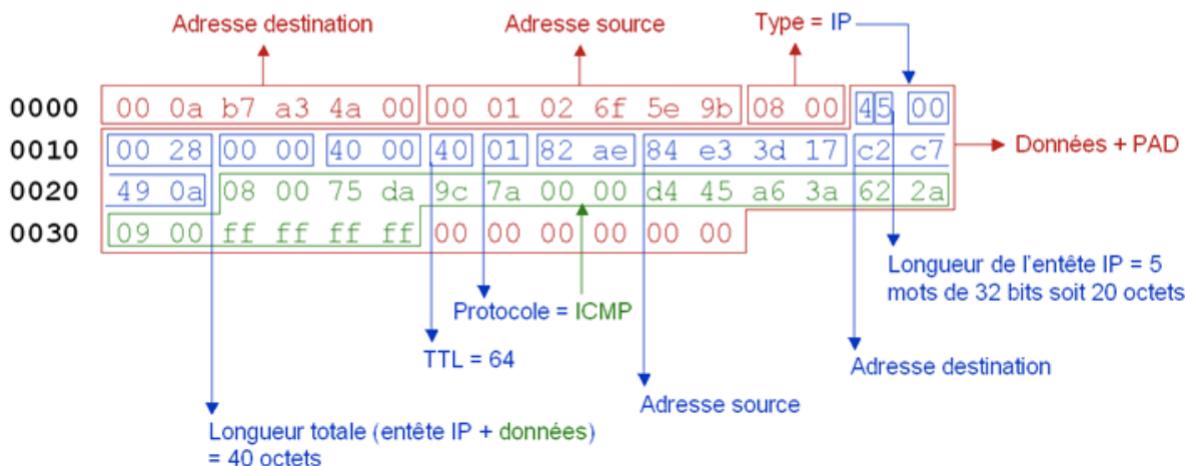
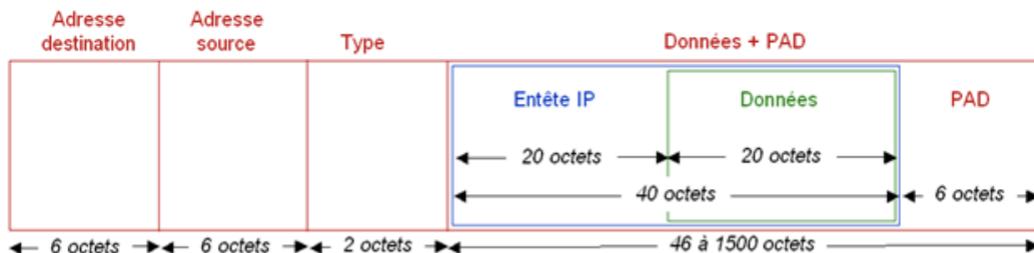
Bloc	Taille	Fonction
Preamble + SFD	8 octets	Synchronisation et délimitation du début de trame
Destination MAC	6 octets	Adresse matérielle du destinataire
Source MAC	6 octets	Adresse matérielle de l'émetteur
EtherType	2 octets	Identification du protocole de couche réseau
Data	46 à 1500 octets	Données utiles
FCS	4 octets	Détection d'erreurs (CRC-32)
Inter Frame Gap	12 octets	Intervalle minimal entre deux trames

Table 2. Structure d'une trame Ethernet II

3. Exercices

3.1 Exercice 1

Un champ sur 2 octets indiquant le type de données encapsulées, et enfin un champ sur au minimum 46 octets contenant les données. Le champ Type valant 0x800, il s'agit de données IP.



Donner les paramètres suivants :

- Adresse IP de la machine ayant initié l'échange
- Adresse MAC de la machine ayant initié l'échange
- Adresse IP de la machine ayant répondu
- Adresse MAC de la machine ayant répondu
- Total Length
- Le protocole encapsulé

3.2 Exercice 2

```
aa aa aa aa aa aa aa ab 00 40 07 03 04 2b 02 60
8c e8 02 91 08 00 45 00 00 2c 14 ee 00 00 3c 06
85 7a 93 d2 5e 63 93 d2 5e 5c 10 a4 09 e7 42 0c
56 01 00 00 00 00 60 02 40 00 c1 29 00 00 02 04
05 b4 02 80 9a b2 5c 48
```

- Que représentent les 8 octets de début ?
- Donner les adresses MAC du destinataire et de l'émetteur ?
- Donner le protocole encapsulé dans la trame ?
- Que représente les 4 octets de la fin ?

3.3 Exercice 3

On a représenté ci-dessous le résultatat d'une capture par Ethereal de trames Ethernet (ni le préambule, ni le FCS ne sont représentés).

Trame 1 :

```
0000  00 12 17 41 c2 c7 00 1a 73 24 44 89 08 00 45 00
0010  00 3c 27 30 00 00 80 01 8f d6 c0 a8 01 69 c0 a8
0020  01 01 08 00 4d 56 00 01 00 05 61 62 63 64 65 66
0030  67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76
0040  77 61 62 63 64 65 66 67 68 69
```

Trame 2 :

```
0000  00 1a 73 24 44 89 00 12 17 41 c2 c7 08 00 45 00
0010  00 3c 00 29 00 00 96 01 a0 dd c0 a8 01 01 c0 a8
0020  01 69 00 00 55 56 00 01 00 05 61 62 63 64 65 66
0030  67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76
0040  77 61 62 63 64 65 66 67 68 69
```

Pour chaque trame, donner les paramètres suivants :

- MAC source
- MAC destination
- Contenu du champ type de protocole
- Version du protocole
- Longueur de l'entête
- Valeur du champ TOS
- Longueur totale du datagramme IP
- Identifiant affecté au d'anagramme
- Valeur des champs DF MF et fragment offset
- En déduire si d'anagramme est fragmenté
- Valeur du champ TTL
- Contenu du champ protocole
- En déduire le protocole encapsulé dans le paquet IP
- Adresse IP source
- Adresse IP destination
- Message ICMP encapsulé dans le d'anagramme IP :
 - valeur du champ type
 - Valeur du champ code
 - Contenu du champ de données du message ICMP

3.4 Exercice 4

On a représenté ci-dessous le résultat d'une capture par le logiciel wireshark d'une trame Ethernet (ni le préambule, ni le FCS ne sont représentés).

Trame

0000	00 12 17 41 c2 c7 00 1a 73 24 44 89 08 00 45 00	...A.... s\$D...E.
0010	01 bb da c2 40 00 3c 06 fc 9d d5 e4 00 2a 3e 93@.<.....*>.
0020	51 3b 00 50 04 85 87 c7 14 d5 00 12 b0 cb 50 19	Q;.P.....P.
0030	19 20 95 45 00 00 3e 20 0a 3c 74 64 20 77 69 64	. .E..> .<td wid
0040	74 86 3d 22 33 30 25 22 20 20 68 65 69 67 68 74	th="30%" height

- Trame Ethernet :
 - Adresse MAC source
 - Adresse MAC Destination
 - Le contenu du champ type de protocole. En déduire le protocole encapsulé dans la trame
- Paquet IP contenu dans la trame Ethernet :
 - La version du protocole
 - La longueur de l'entête
 - La valeur du champ TOS
 - La longueur totale du datagramme IP
 - L'identifiant affecté au datagramme
 - La valeur des champs DF, MF et fragment offset. En déduire si datagramme est fragmenté
 - La valeur du champ TTL
 - Le contenu du champ protocole. En déduire le protocole encapsulé dans le paquet IP
 - Les adresses IP source et destination
- Segment TCP encapsulé dans le datagramme IP :
 - La valeur du champ type et du champ code. En déduire la nature du message ICMP
 - Le contenu du champ de donnée du message ICMP

3.5 Exercice 5

Donner les différents paramètres des trames suivantes :

Trame 1

0000	f8 32 e4 9c f3 b3 f0 7f 06 ae 4c c0 08 00 45 00	.2.....L...E.
0010	33 ff 2a 9c 40 00 3d 06 79 61 0a 65 80 18 0a 65	3.*.@.=.ya.e....e
0020	d1 19 00 50 80 fe 78 63 0f 7b 08 17 40 10 80 18	...P..xc.{...@...}
0030	00 fc 99 ed 00 00 01 01 08 0a 06 bf 30 64 7c 850d .
0040	30 9f 48 54 54 50 2f 31 2e 31 20 32 30 30 20 4f	0.HTTP/1.1 200 0
0050	4b 0d 0a 43 6f 6e 74 65 6e 74 2d 54 79 70 65 3a	K..Content-Type:
0060	20 74 65 78 74 2f 68 74 6d 6c 0d 0a 43 6f 6e 74	text/html..Cont

Trame 2

0000	33 33 00 00 00 16 do 23 db 54 8f 2a 86 dd 60 00	33.....#.T.*...`.
0010	00 00 00 38 00 01 00 00 00 00 00 00 00 00 00 008.....
0020	00 00 00 00 00 00 ff 02 00 00 00 00 00 00 00 00 00
0030	00 00 00 00 00 16 3a 00 01 00 05 02 00 00 8f 00:
0040	9c a2 00 00 00 02 04 00 00 00 ff 02 00 00 00 00 00
0050	00 00 00 00 00 02 6f d3 d0 7b 04 00 00 00 ff 02o...{.....
0060	00 00 00 00 00 00 00 01 ff 54 8f 2aT.*

Trame 3

0000	ff ff ff ff ff d0 23 db 54 8f 2a 08 06 00 01#.T.*....
0010	08 00 06 04 00 01 d0 23 db 54 8f 2a c0 a8 87 ca#.T.*....
0020	00 00 00 00 00 00 c0 a8 87 fe 00 00 00 00 00 00
0030	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Trame 4

0000	00 14 6c 39 26 3c c8 9c dc bd b4 1f 08 00 45 00	..19&<.....E.
0010	00 54 00 00 40 00 40 01 a2 da c0 a8 87 19 c0 a8	.T..@.@.....
0020	8f 64 08 00 8a 11 0a 7e 00 01 bc 00 91 4f 00 00	.d.....~.....0..
0030	00 00 54 4c 03 00 00 00 00 00 10 11 12 13 14 15	..TL.....
0040	16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25 !"#\$%
0050	26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35	&'()*,-./012345
0060	36 37	

Trame 5

0000	33 33 00 01 00 02 cc af 78 1a 2c 53 86 dd 60 00	33.....x.,S...`.
0010	00 00 00 64 11 01 fe 80 00 00 00 00 00 00 85 e8	...d.....
0020	05 2c df 4a 60 d0 ff 02 00 00 00 00 00 00 00 00 00	.,.J`.....
0030	00 00 00 01 00 02 02 22 02 23 00 64 68 ae 01 9f".#.dh...
0040	da 5c 00 08 00 02 05 dc 00 01 00 0e 00 01 00 01	.\\.....
0050	15 97 8c 4f b8 70 f4 a3 9c c4 00 03 00 0c 17 cc	...0.p.....
0060	af 78 00 00 00 00 00 00 00 00 27 00 0e 00 0c	.x.....!....
0070	53 6c 61 76 6f 2d 4c 61 70 74 6f 70 00 10 00 0e	Slavo-Laptop....
0080	00 00 01 37 00 08 4d 53 46 54 20 35 2e 30 00 06	...7..MSFT 5.0..
0090	00 08 00 18 00 17 00 11 00 27!

1. Annexes

A.1 Trame IPV4

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Version	IHL	Type Of Service	ECN	Total Length																											
Identification		0		DF	MF	Fragment Offset																									
Time to live	Protocol	Header Checksum																													
Source IP address		Destination IP address																													
Option + Padding 0 to 40 bytes		DATA																													
...																															

IPV4
Header

Version : numéro de version du protocole IP

- 04 - IP V4
- 05 - ST Datagram Mode
- 06 - IP V6

IHL (Internet header length) : longueur de l'entête IP

Service : gestion d'une qualité de service traitée (Priorité, Délai, Débit, Fiabilité, ...)

Longueur totale : longueur du paquet incluant l'entête IP et les Data
 Identification : identification pour reconstituer les différents fragments
 Flags : état de la fragmentation. Voici le détail des différents bits constituant ce champ.

- DF : Don't Fragment
- MF : More Fragments
- le troisième bit indique si le fragment est le dernier

Position fragment : indique la position du fragment par rapport à la première trame

TTL (Time To Live) : indique la durée de vie maximale du paquet

Protocole : représente le type de Data :

- 1 - 00000001 - 0x01 - ICMP
- 2 - 00000010 - 0x02 - IGMP
- 4 - 00000100 - 0x04 - IP
- 6 - 00000110 - 0x06 - TCP
- 17 - 00010001 - 0x11 - UDP
- 27 - 00011011 - 0x1B - RDP
- 41 - 00101001 - 0x29 - IPV6
- 50 - 00110010 - 0x32 - ESP
- 51 - 00110011 - 0x33 - AH
- 58 - 00111010 - 0x3A - IPV6-ICMP

Checksum : représente la validité du paquet de la couche 3

Adresse IP source : adresse IP source ou de réponse

Adresse IP destination : adresse IP destination

Options : optionnel

Bourrage : permet de combler le champ option

A.2 Trame IPV6

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31								
Version	Trafic Class	Flow Label																																					
Payload Length										Next Header			Hop Limit																										
Source IP address (128 bits)																																							
...																																							
Destination IP address (128 bits)																																							
...																																							

A.3 Trame UDP

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31																			
Source Port																Destination Port																																		
Length																Checksum																																		
Application Layer Data (0 Octets ou plus)																																																		
...																																																		

A.4 Trame TCP

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31										
Source Port																Destination Port																									
Sequence Number																Acknowledgement Number																									
Data Offset	Reserved	URG	ACK	PSH	RST	SYN	FIN	Window																Urgent Pointer																	
Checksum																Options																									
...																																									
Data (Optional)																...																									

Port source : port relatif à l'application sur la machine source.

Port destination : port relatif à l'application sur la machine de destination.

Numéro de séquence : numéro du paquet.

Numéro de l'accusé de réception : acquittement pour les paquets reçus.

Offset : indique donc où les données commencent.

Réservé : pour des besoins futur.

Flags :

- URG : champ Pointeur de donnée urgente est utilisé.
- ACK : numéro de séquence pour les acquittements est valide.
- PSH : indique au récepteur de délivrer les données à l'application
- RST : demande la réinitialisation de la connexion.
- SYN : indique la synchronisation des numéros de séquence.
- FIN : indique fin de transmission.

Fenêtre : nombre d'octets à partir de la position marquée dans l'accusé de réception que le récepteur est capable de recevoir.

Checksum : validité du paquet de la couche 4 TCP.

Pointeur de donnée urgente : position d'une donnée urgente en donnant son décalage par rapport au numéro de séquence.

Options : optionnel.

Bourrage : permet de combler le champ option.

22	ssh	123	ntp
23	telnet	143	imap
25	smtp	161	snmp
53	dns	162	snmptrap
67	dhcp Server/Relay	443	https
68	dhcp client	546	Dhcp-v6 Client
69	tftp	547	Dhcp-v6 Server/Relay
80	http		

A.5 Trame ARP/RARP

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31																									
Hardware Type																Protocol Type																																								
Hardware Add Len								Protocol Add Len								Reserved (Opcode)																																								
Sender Hardware Address																																																								
Sender Hardware Address																Sender Protocol Address																																								
Sender Protocol Address																Target Hardware Address																																								
Target Hardware Address																																																								
Target Protocol Address																																																								

Opération :

- 1 ARP request.
- 2 ARP response.
- 3 RARP request.
- 4 RARP response.

A.6 Trame ICMP

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	
Type																Checksum																
Identifier																Sequence Number																
Address Mask																																

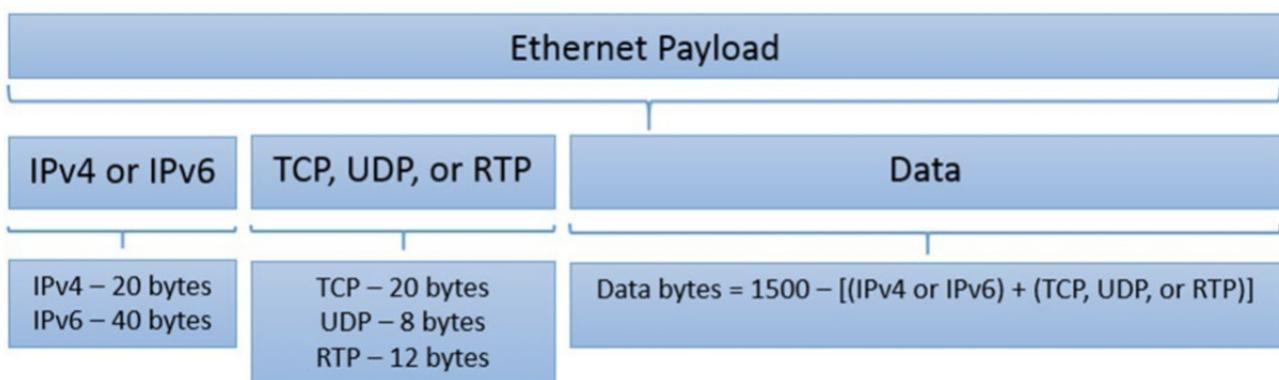
Type	Code	Description
0		Echo reply
3		Destination unreachable
3	0	Net unreachable
3	1	Host unreachable
3	2	Protocol unreachable
3	3	Port unreachable
5		Redirect
5	0	Redirect datagrams for the network
5	1	Redirect datagrams for the host
5	2	Redirect datagrams for the type of service and network
5	3	Redirect datagrams for the type of service and host
8		Echo. (request)
11		Time exceeded
11	0	Time to live exceeded in transit
135	0	Neighbor Solicitation
135	0	Neighbor advertisement

A.7 Trame ICMPv6

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Type		Code		Checksum																											

A.8 Charge utile Ethernet

La charge utile Ethernet varie en fonction du type de données qu'elle transporte. Il s'agit d'une combinaison d'en-têtes TCP, UDP ou RTP combinés à un en-tête IPv4 ou IPv6, et surtout de la charge utile réelle qui contient les données envoyées. Les champs de la charge utile sont affichés dans la figure suivante :



Comme le montre la figure, la quantité de données réelles envoyées dans une trame Ethernet dépend du nombre d'octets consommés par les autres champs. D'autres options sont disponibles qui ne sont pas listées ici. Par exemple, les hôtes Linux ajoutent automatiquement un horodatage à la pile TCP, ajoutant 12 octets.