Structure de trame Ethernet

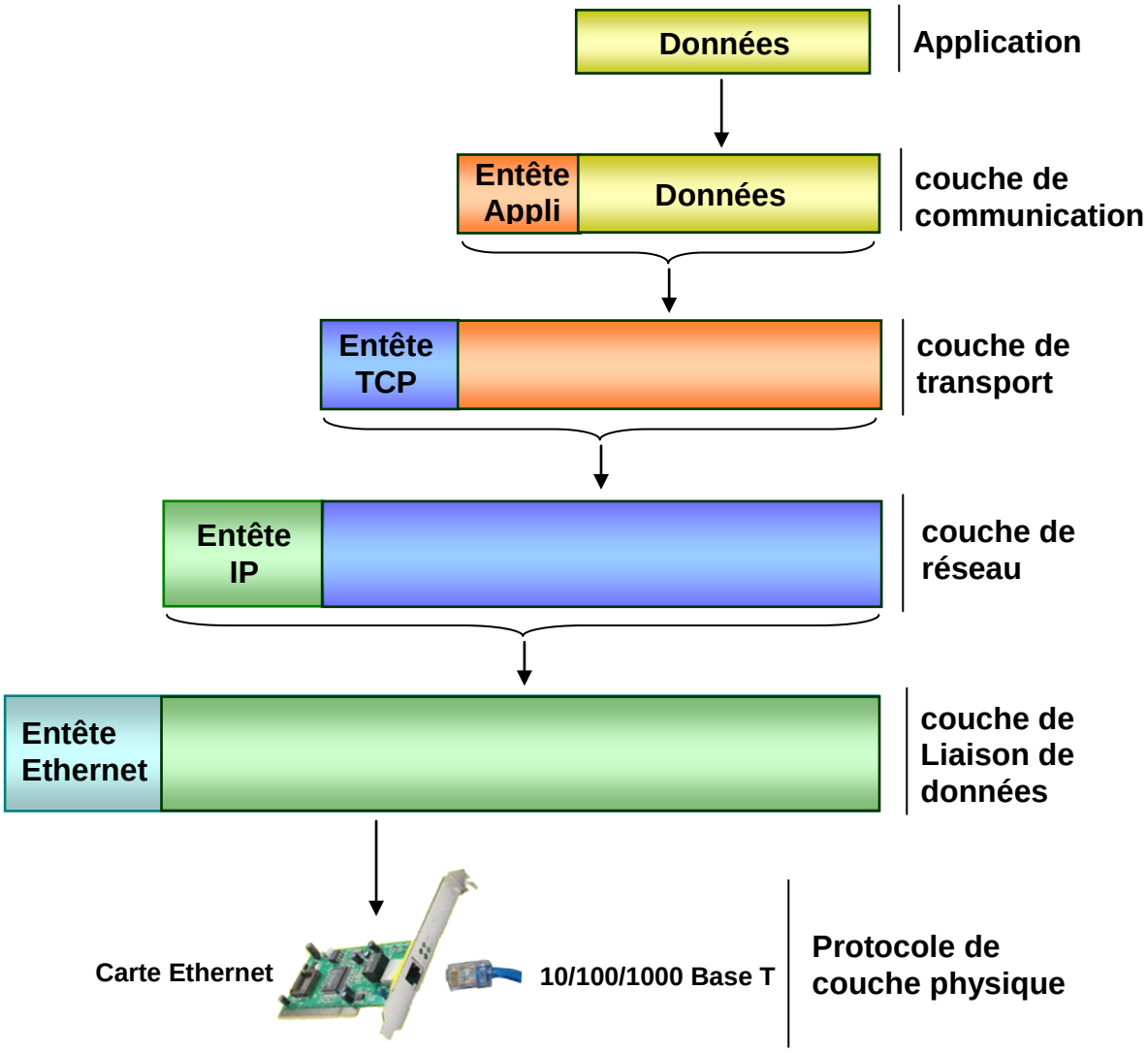
Normalisation

Le format des trames Ethernet est défini par la norme internationale IEEE 802.2/802.3 (Institute of Electrical and Electronics Engineers) La norme 802.3 définit la structure de trame Ethernet.

La trame Ethernet est le produit de l'encapsulation des données de protocole de la couche OSI.

Encapsulation des données de protocoles

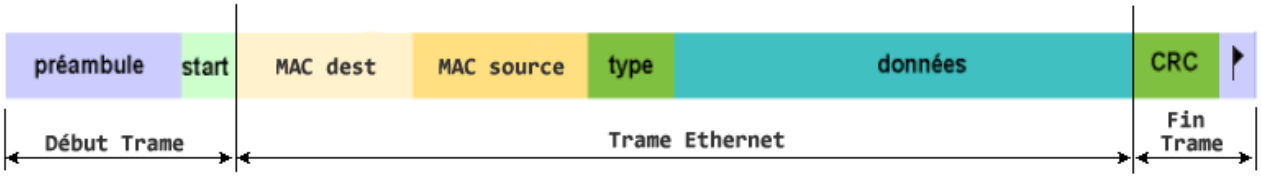
Dans un réseau Ethernet, la transmission de données utilise le format de trames 802.3. Chaque couche encapsule les données de la couche supérieure et ajoute ses propres données.



Nota : L'ensemble des données encapsulées (entête + données) sont transmises par la carte Ethernet dans une trame.

Trame Ethernet

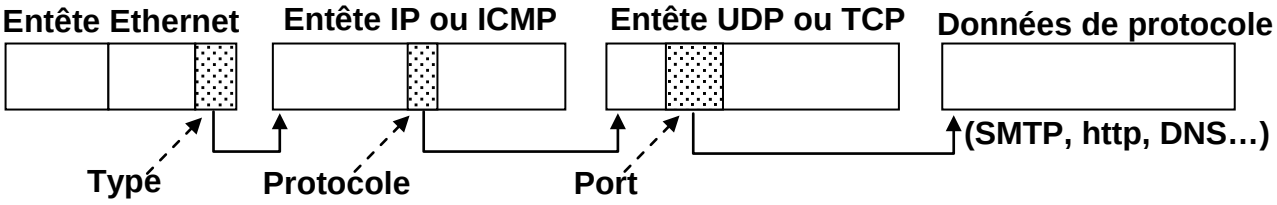
Les données sont envoyées dans la carte qui constitue la trame pour la transmettre sur le réseau. La trame Ethernet comprend un motif de début de trame et une séquence de contrôle FCS en fin de trame.



Les données CRC (4 octets) permettent de vérifier la trame à la réception et de s'assurer de l'intégrité du contenu de la trame.
L'entête et la fin de trame FCS appartiennent à la couche physique du modèle OSI.

Procédure pour l'analyse de trame

Une trame Ethernet est constituée de plusieurs blocs. Chaque bloc contient les informations de protocole propres à chaque couche. Chaque bloc contient une information qui indique la nature du bloc suivant et, par conséquent, la structure de ce bloc ce qui permet de le décrypter.



L'objectif est donc d'analyser bloc par bloc le contenu des données d'une trame afin d'en retirer les informations qui vont permettre de comprendre la signification de celle-ci.

Entête de couche 2 Ethernet 802.3

Entête Ethernet MAC 802.3

OCTET 1	OCTET 2	OCTET 3	OCTET 4
MAC Destination			
MAC Destination		**MAC Source**	
MAC Source			
TYPE			

Le tableau ci-dessous présente la liste non exhaustive des principaux protocoles utilisés et codés dans le champ TYPE.

TYPE (Hexa)	PROTOCOLE
0800	**Trame IP**
0806	**ARP**
8100	**Trame 802.1Q**
- - -	- - -
809B	AppleTalk
8863	PPPoE

Entête de couche 2 Ethernet 802.1Q

Entête Ethernet MAC 802.1Q

	OCTET 1	OCTET 2	OCTET 3	OCTET 4
	MAC Destination			
	MAC Destination		MAC Source	
	MAC Source			
TAG	E/TYPE (8100)		PRI / CFI	VLAN ID
	TYPE			

!!! Cette entête est particulière. Elle n'est utilisée que dans le cas d'un réseau structuré en réseaux virtuels VLAN.

Structure de l'Entête de couche 3 réseau IP

Entête IP			
OCTET 1	OCTET 2	OCTET 3	OCTET 4
Version	Type de service	Longueur Entête	
Identificateur		Fragmentation	
TTL	Protocole	Contrôle	
IP Source			
IP Destination			

L'entête IP contient en particulier les informations qui désignent la version de la trame IP (IPV4 ou IPV6) la durée de vie d'un paquet (TTL) le protocole de transport le type de service et les adresses IP source et destination.

Le champ Type de service désigne le type de données transportées dans le paquet. Ces données peuvent être de la voix, Vidéo, données numériques. Ce champ permet de définir la priorité à donner au traitement du paquet.

Le champ protocole donne le type de protocole de transport en charge des données. Ce champs détermine la structure de trame de transport.

Le tableau ci-dessous présente la liste des protocoles possibles présents dans le champ protocole de l'entête IP.

Protocole (Hexa)	Nom	Description
01	**ICMP**	**Protocole de contrôle des messages (unicast)**
06	**TCP**	**Protocole de transport des messages en mode sécurisé**
11	**UDP**	**Protocole de transport des messages simplifié sans connexion**
17	**IGMP**	**Protocole de contrôle des messages (multicast)**
- - -	- - -	- - -
27	RDP	Protocole de transport fiable
05	ST	Protocole de transport de streaming

Entête TCP

OCTET 1	OCTET 2	OCTET 3	OCTET 4
Port Source		Port destination	
N° d'ordre			
Numéro d'accusé réception			
Padding	réservé	URG ACK PSH RST SYN FIN	Fenêtre
Somme Contrôle		Pointeur urgence	
Options			Remplissage

Etat TCP déconnecté : **0 0 0 0 0 0**
Etat TCP établi : **0 1 0 0 1 0** **(Ack=1, SYN=1)**

Entête UDP

OCTET 1	OCTET 2	OCTET 3	OCTET 4
Port Source		Port destination	
Longueur		Contrôle	

Les entêtes TCP et UDP contiennent les informations qui identifient les applications (port source et port destination).

Un port client est ouvert par un poste utilisateur qui se connecte à un serveur identifié par un port public.

Tableau des protocoles de communication

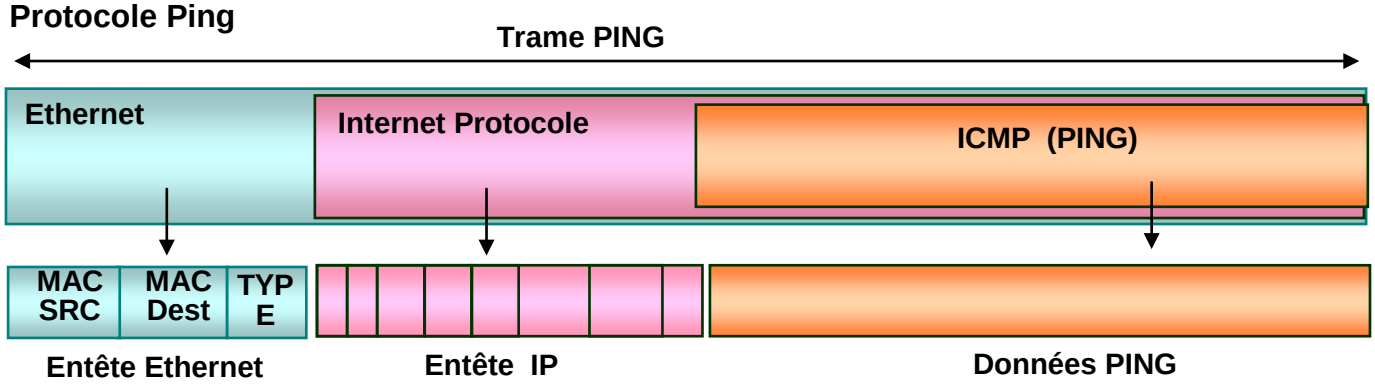
La table ci-dessous décrit la liste des principales applications de communication, les ports et les protocoles de communication associés.

Protocoles de communication	N° PORT (Décimal)	Protocole Transport	Protocole Réseau	Description
PING	- - -	ICMP	IP	Test de connectivité
FTP	20, 21	TCP	IP	Protocole de transfert de fichier
SSH	22	TCP	IP	Protocole de connexion à distance sécurisé
TELNET	23	TCP	IP	Protocole de connexion à distance
SMTP	25	TCP	IP	Protocole pour le serveur d'émission messagerie
POP3	110	TCP	IP	Protocole pour le serveur de réception messagerie
IMAP	143	TCP	IP	Protocole pour le serveur de messagerie enrichie (remplace SMTP et POP)
DNS	53	UDP	IP	Serveur de nom de domaine
DHCP	67	UDP	IP	Serveur DHCP
DHCP	68	UDP	IP	Client DHCP
HTTP	80	TCP	IP	Protocole d'accès au service WEB
LDAP	389	TCP	IP	Protocole utilisé par les serveurs d'annuaire Active Directory ou Open LDAP sous Linux
HTTPS	443	TCP	IP	https (sécurisé avec SSL ou TLS)
SIP	5060	TCP	IP	Protocole de signalisation VoIP
RTP	60200	UDP	IP	Protocole de Transport de la voix VOIP
RADIUS	1812, 1813	UDP	IP	Protocole d'authentification

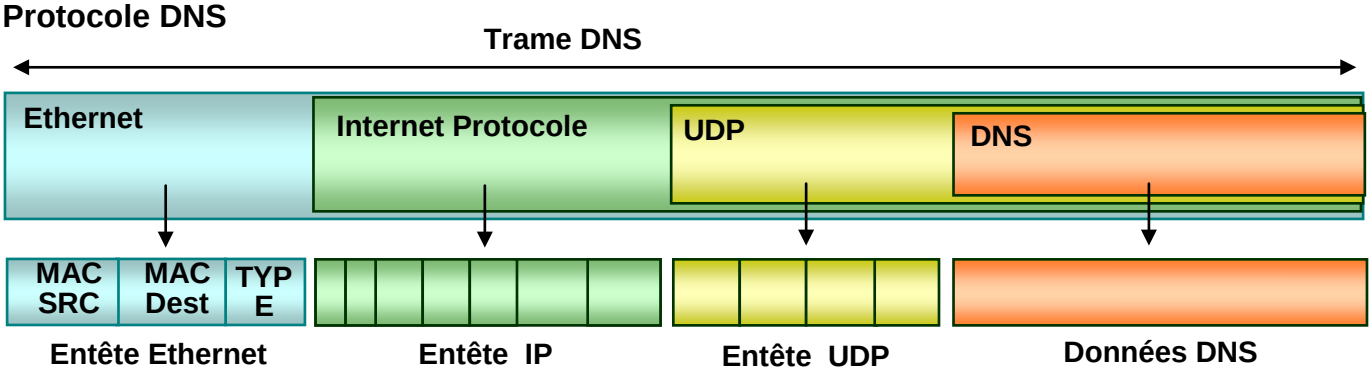
!!! Attention, les valeurs de port ci-dessus sont exprimées en décimal.

Format des principales trames de communication

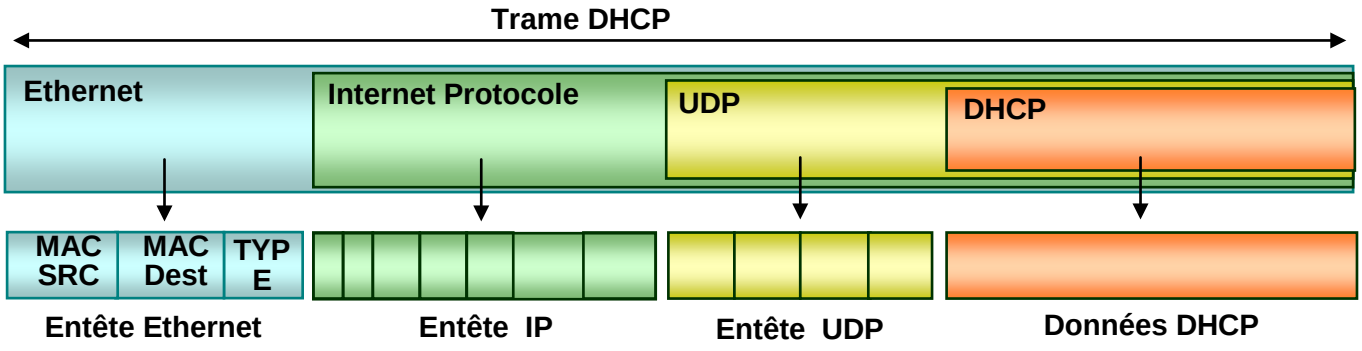
Protocole Ping



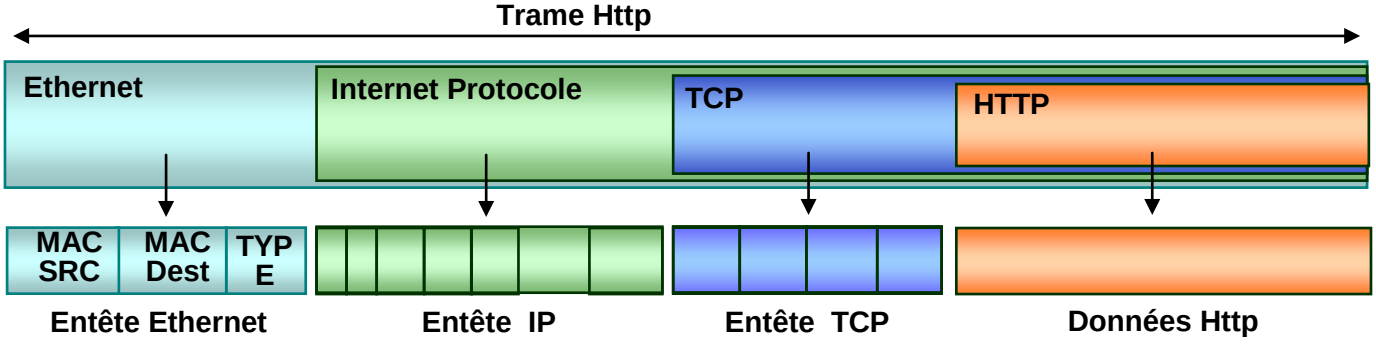
Protocole DNS



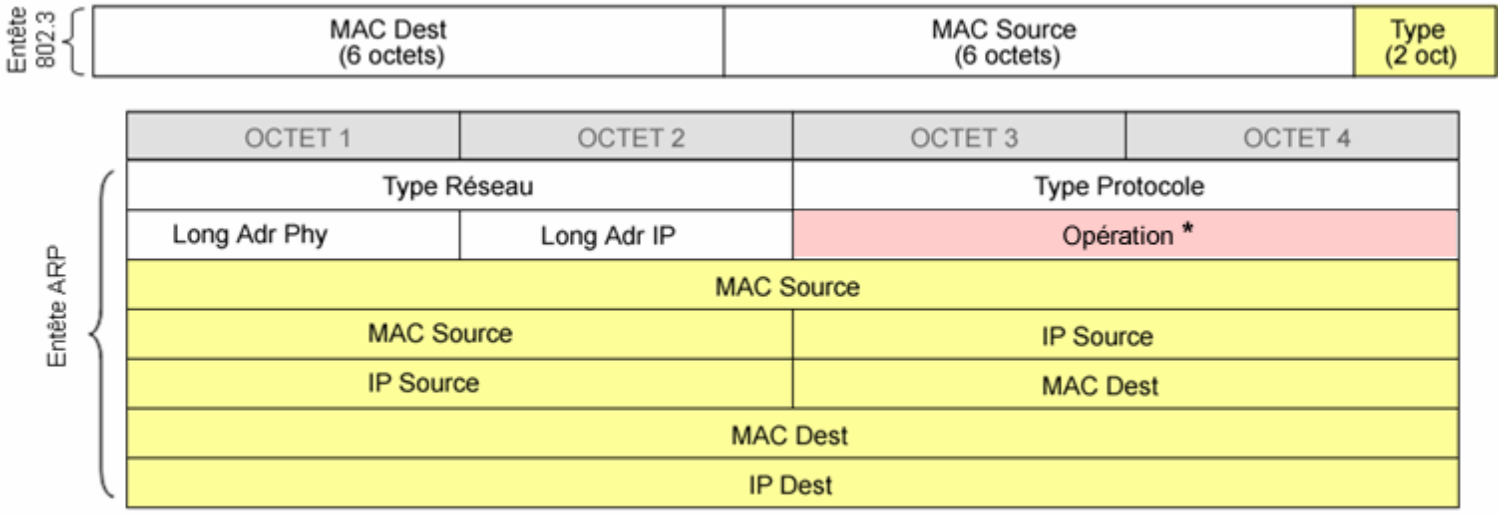
Protocole DHCP



Protocole Http

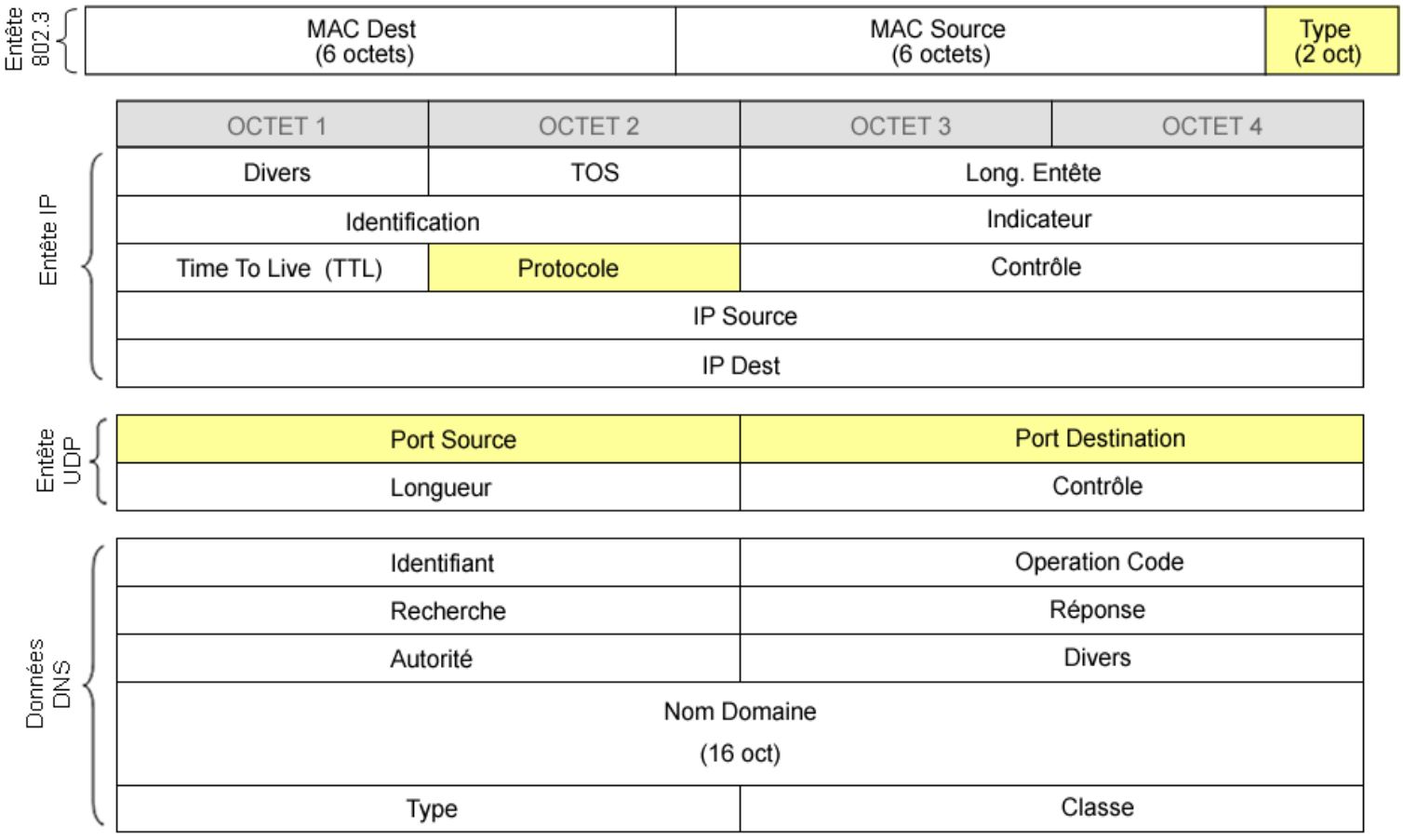


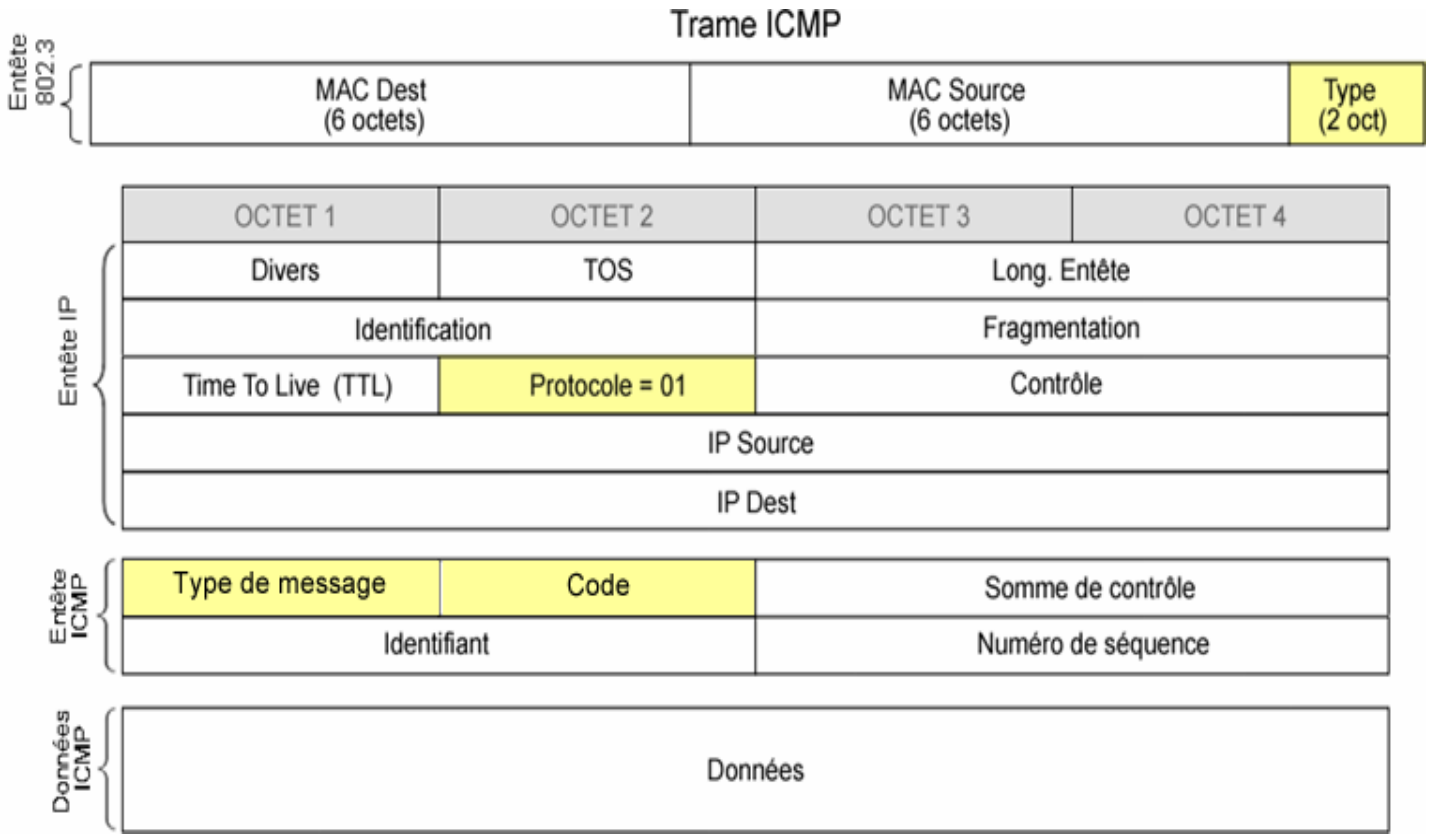
Trame ARP



* Opération : 01 - Request
02 - Reply

Trame DNS





* Protocole : dans le cas ICMP protocole = 01.

La trame ICMP est utilisée pour tester la connectivité entre équipements et informer la cause de la tentative réussie ou échouée de cette communication.

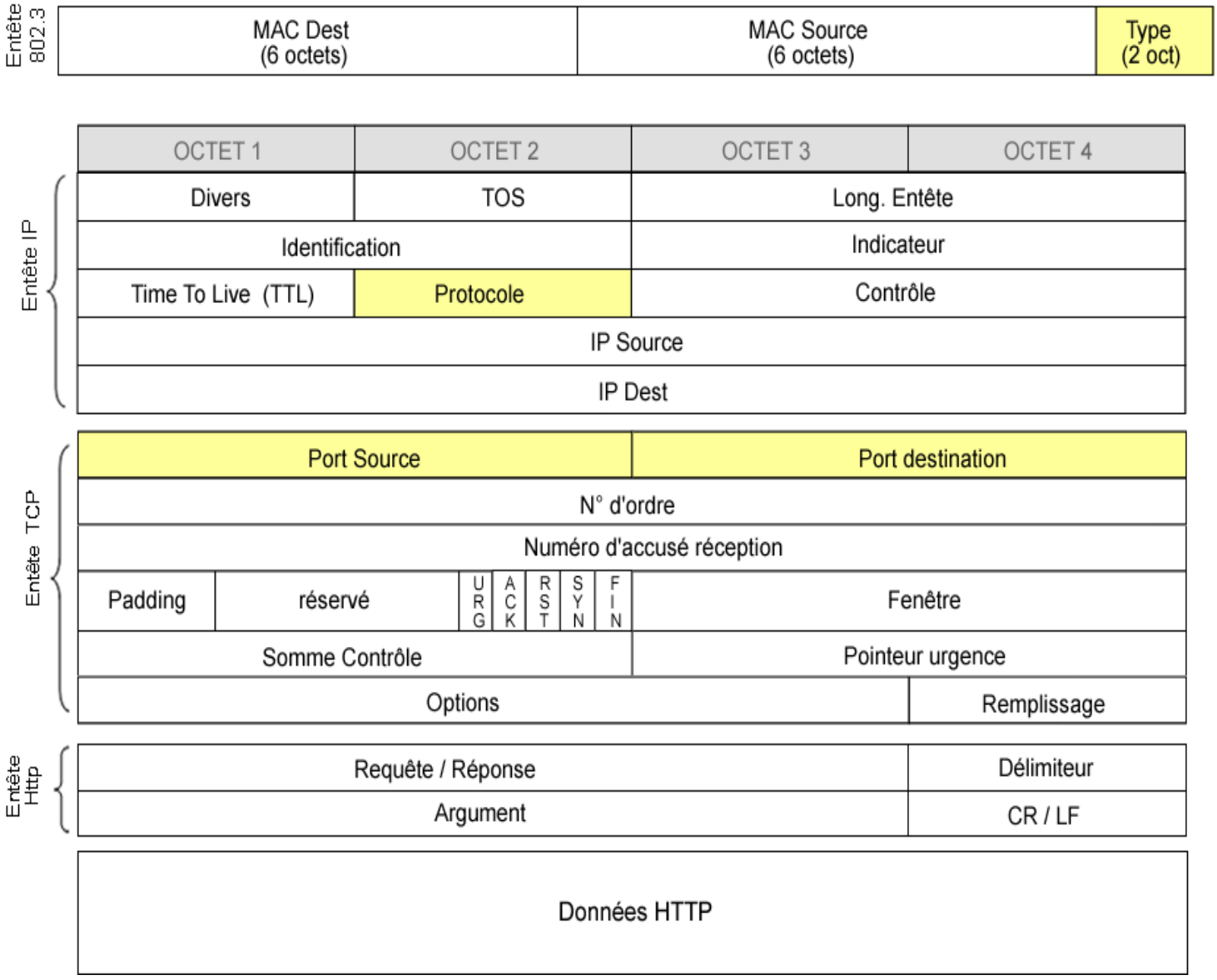
Les informations contenant les résultats sont contenues dans les champs Type de message et Code de message de la trame ICMP (Voir tableau ci-dessous).

Les données ICMP sont des informations internes au protocole ICMP et ne sont pas prises en compte dans les analyses.

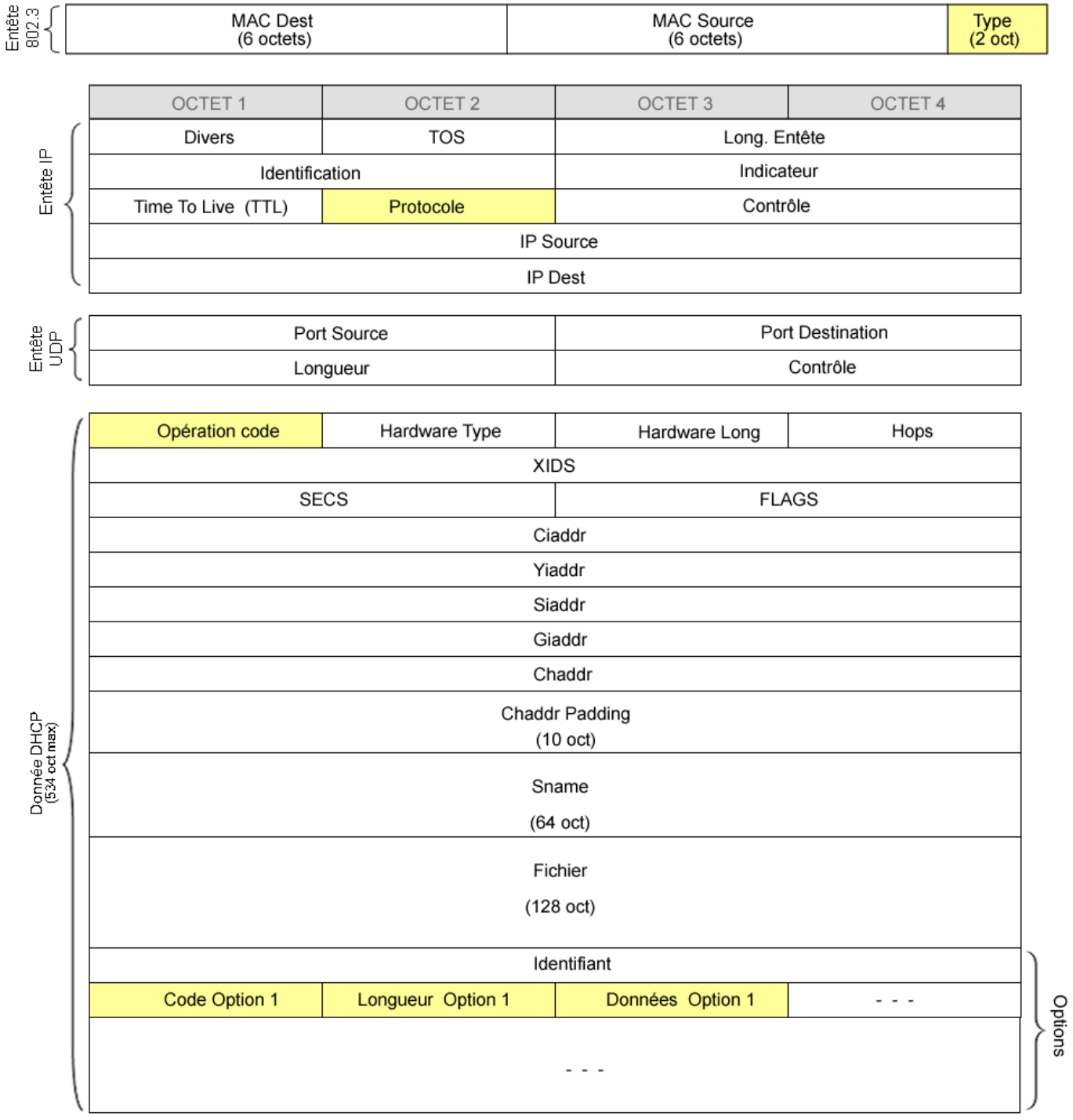
Tableau causes ICMP

Type	Code	Cause
0	0	Réponse à une demande d'écho
3	0	Réseau inaccessible
3	1	Hôte inaccessible
3	2	Protocole inaccessible
3	3	Port inaccessible
3	5	Echec de routage par la source
3	6	Réseau de destination inconnu
3	7	Hôte de destination inconnue
3	8	Machine source isolée
3	9	Réseau de destination interdit administrativement
3	10	Hôte de destination interdite administrativement
3	11	Réseau inaccessible pour ce type de service
3	12	Hôte inaccessible pour ce type de service
3	13	Communication interdite par un filtre
4	0	Volume de donnée trop importante
5	0	Redirection pour un hôte
5	1	Redirection pour un hôte et pour un service donné
5	2	Redirection pour un réseau
5	3	Redirection pour un réseau et pour un service donné
8	0	Demande d'écho
9	0	Avertissement routeur
10	0	Sollicitation routeur
11	0	Durée de vie écoulée avant d'arrivée à destination
11	1	Temps limite de réassemblage du fragment dépassé
12	0	En-tête IP invalide
12	1	Manque d'une option obligatoire
15	0	Demande d'adresse réseau
16	0	Réponse d'adresse réseau
17	0	Demande de masque de sous réseau
18	0	Réponse de masque de sous réseau

Trame HTTP


Entête 802.3
MAC Dest (6 octets)
MAC Source (6 octets)
Type (2 oct)
OCTET 1
OCTET 2
OCTET 3
OCTET 4
Entête IP
Divers
TOS
Long. Entête
Identification
Indicateur
Time To Live (TTL)
Protocole
Contrôle
IP Source
IP Dest
Entête TCP
Port Source
Port destination
N° d'ordre
Numéro d'accusé réception
Padding
réservé
URG
ACK
RST
SYN
FIN
Fenêtre
Somme Contrôle
Pointeur urgence
Options
Remplissage
Entête Http
Requête / Réponse
Délimiteur
Argument
CR / LF
Données HTTP

Trame DHCP



- Opération code : 01 : désigne une requête ; 02 : désigne une réponse
- Ciaddr : adresse IP du client, lorsqu'il en a déjà une, Yiaddr : la nouvelle adresse IP du client,
- Siaddr : adresse IP du (prochain) serveur à utiliser, Giaddr : adresse IP du relais,
- Chaddr : adr MAC client

Options : permet de définir le type de message envoyé (- code option 53 (décimal) : détermine le type de message transmis → Données options : (Discover=1 ; Offer=2 ; Request=3 ; Ack=5 ; release=7 ; Inform=8…)

Tableau des principaux Codes Options DHCP

CODE Décimal (Hexa)	TYPE	DESCRIPTION
1 (1)	**Masque de sous réseau**	**Donne le masque au client (4 octets)**
3 (3)	**Routeur**	**Donne l'adresse de la passerelle (4 octets)**
4 (4)	Serveur NTP	Donne l'adresse du serveur de temps NTP (4 octets)
6 (6)	**Serveur DNS**	**Donne l'adresse du serveur DNS préféré (4 octets)**
12 (C)	**Hostname**	**Nom de machine**
28 (1C)	Adresse de diffusion	Donne l'adresse de diffusion dans le sous réseau (4 octets)
43 (2B)	Vendor-Specific-Information	Info privée du Fabricant
50 (32)	**Requested IP address**	**@IP client préférée**
51 (33)		
53 (35)	**Type de message**	**Discover, Offer, Request, Ack**
54 (36)	**DHCP server Identifier**	**@IP Serveur DHSP**
55 (37)	Parameter Request list	Liste des paramètres demandés
60 (3C)	Vendor Class Identifier	
61 (3D)	Client identifier	Constructeur Hardware
69 (45)	Serveur SMTP	Donne l'adresse du serveur SMTP (4 octets)
70 (46)	Serveur POP3	Donne l'adresse du serveur POP3 (4 octets)
150 (96)	Adresse serveur TFTP	Donne l'adresse du serveur TFTP (4 octets)