UNIVERSITE D'EVRY
VAL D'ESSONNE

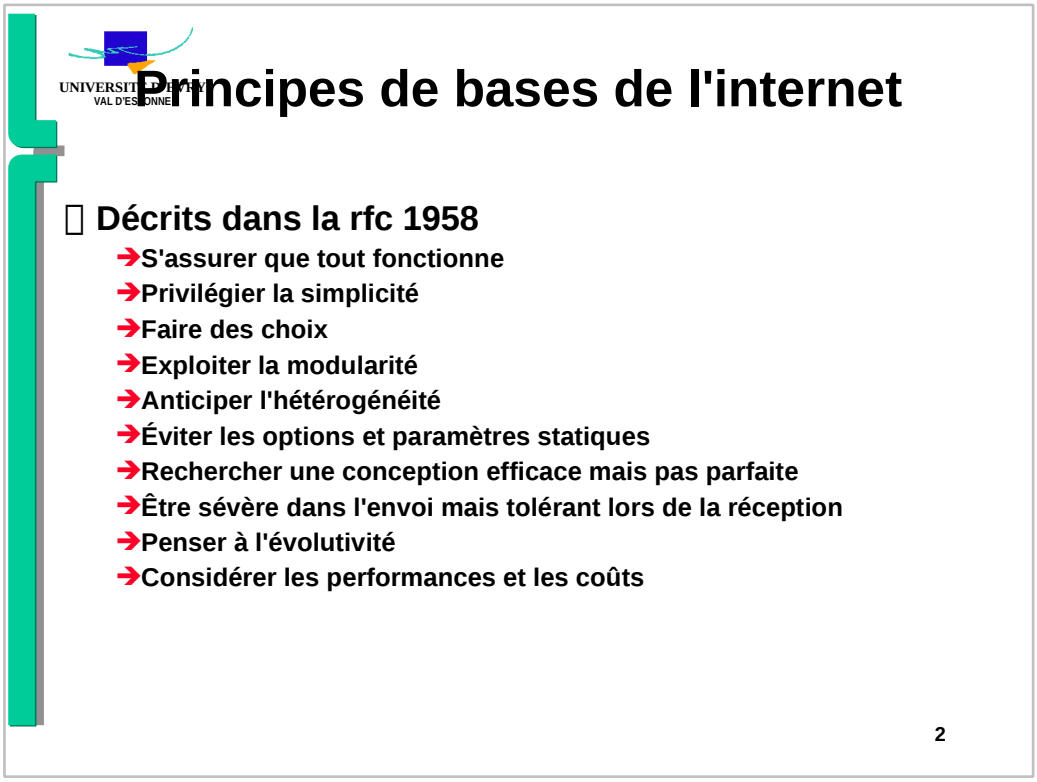
INTERNET PROTOCOL

IPv4

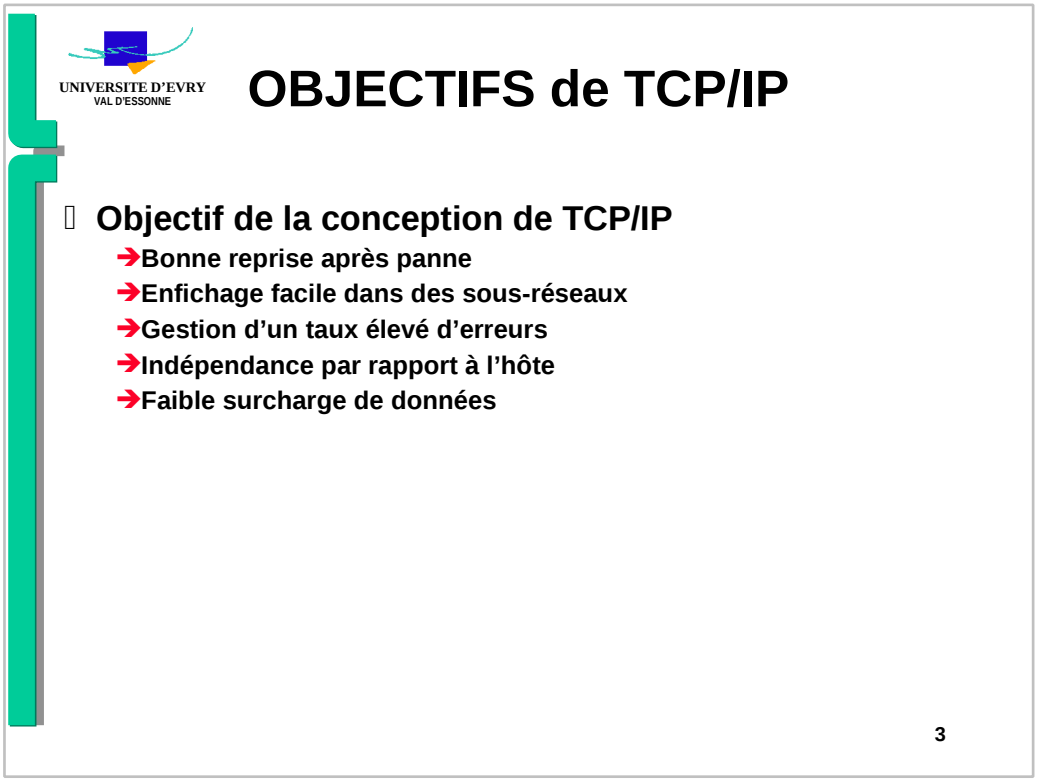
Module Détaillé

document d'origine: **Michel BESSON**
évolutions: P. Petit

1



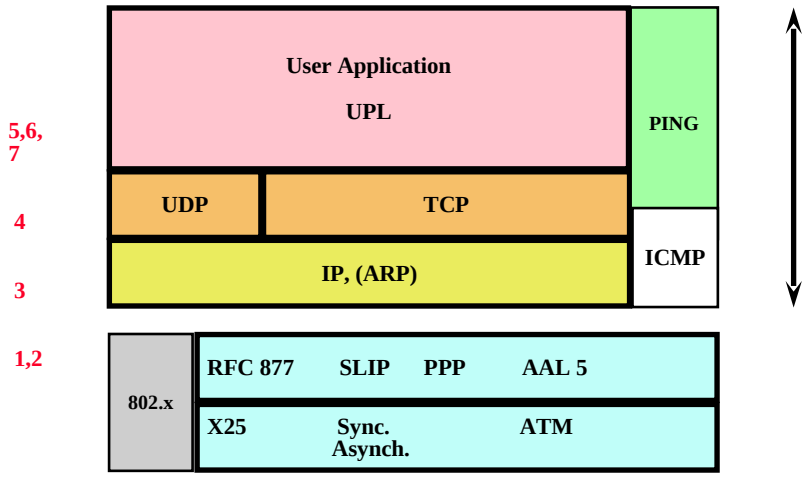
- **Objectifs initiaux relatifs à la conception de TCP/IP**
  - **Bonne reprise après panne**
    - **Adapté à un contexte de défense (fonctionne même après des destructions importantes de liens et sites).**
  - **Enfichage facile dans des sous-réseaux**
    - **Peut être reconstruit à partir de réseaux existant ou nouveaux**
  - **Gestion d'un taux élevé d'erreurs**
    - **Support d'erreurs prévisibles et non prévisibles avec un résultat satisfaisant à 100% (erreurs liées à la qualité des supports ou à leur destruction)**
  - **Indépendance par rapport à l'hôte**
    - **Non dédié à un quelconque fournisseur**
  - **Faible surcharge de données**
    - **Les concurrents TP4 et X25 utilisent des en-tête fixes et variables plus lourdes**



- **Objectifs initiaux relatifs à la conception de TCP/IP**
  - **Bonne reprise après panne**
    - **Adapté à un contexte de défense (fonctionne même après des destructions importantes de liens et sites).**
  - **Enfichage facile dans des sous-réseaux**
    - **Peut être reconstruit à partir de réseaux existant ou nouveaux**
  - **Gestion d'un taux élevé d'erreurs**
    - **Support d'erreurs prévisibles et non prévisibles avec un résultat satisfaisant à 100% (erreurs liées à la qualité des supports ou à leur destruction)**
  - **Indépendance par rapport à l'hôte**
    - **Non dédié à un quelconque fournisseur**
  - **Faible surcharge de données**
    - **Les concurrents TP4 et X25 utilisent des en-tête fixes et variables plus lourdes**

UNIVERSITE D'EVRY
VAL D'ESSONNE

MODELE TCP/IP



4

UNIVERSITE D'EVRY
VAL D'ESSONNE

Architecture de IP

COMPOSANTS DE NIVEAU 3

- **ICMP : Internet Control Message Protocol**
- **IP : Internet Protocol**
- **ARP : Address Resolution Protocol**

5

UNIVERSITE D'EVRY
VAL D'ESSONNE

Architecture de IP

IP
Internet Protocol

Assure la transmission en mode DATAGRAMME

Fragmentation et réassemblage des paquets

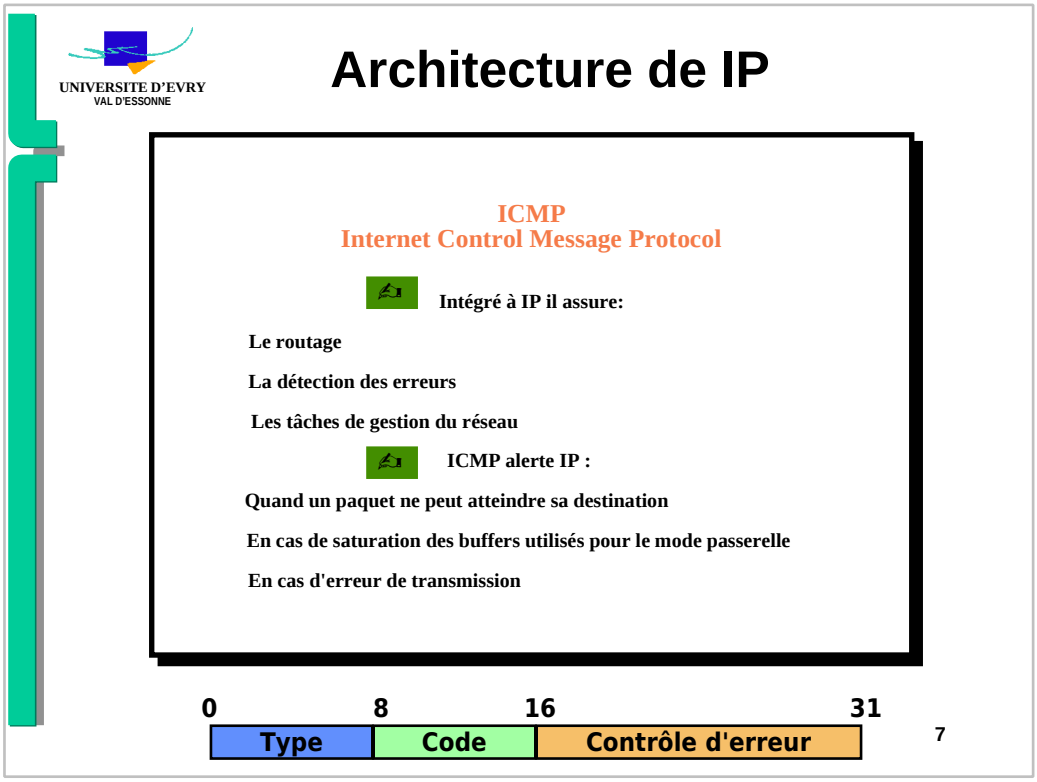
Détermination de la route d'acheminement

Interface avec les protocoles supérieurs (TCP, UDP)

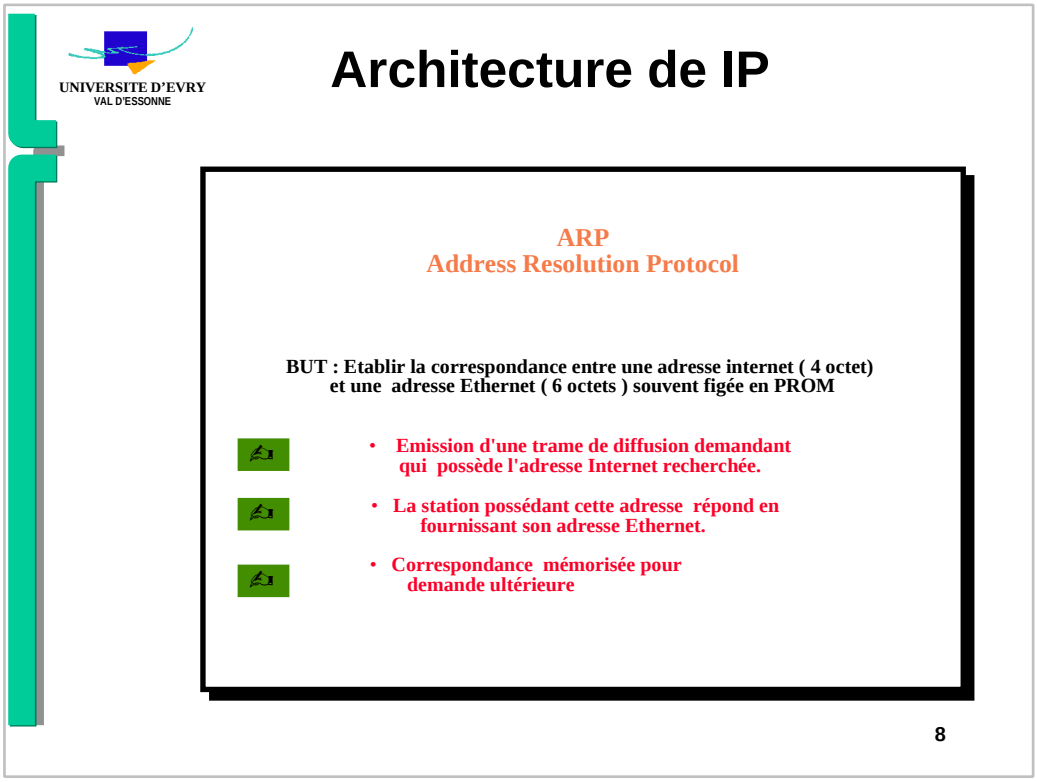
Interface avec la couche de niveau 2 (via ARP)

Fonction de passerelle

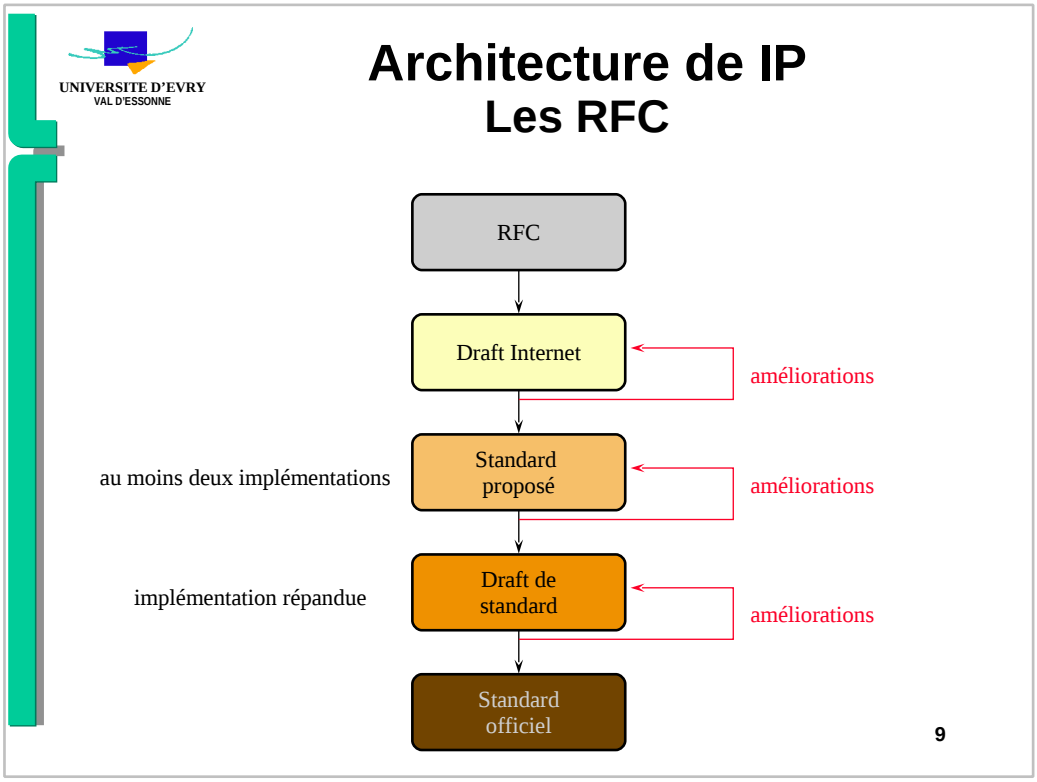
6



- **SYNTHESE DES MESSAGES D'ICMP**
  - **Ils comprennent et indiquent:**
    - **Destination inaccessible**
      - **réseau ou machine inaccessibles ou bien encore ...**
      - **protocole non utilisé, fragmentation nécessaire (si interdite par flag)**
    - **Durée excessive**
      - **fragment à TTL épuisé, ou présent dans un queue "durée de réassemblage excessive"**
    - **Problème de paramètre :** erreur dans un en-tête IP
    - **Demande de réduction de débit de la source**
      - **un équipement détruit les datagr. car tampons épuisés**
    - **Redirection:** Indique à une machine l'adresse d'un routeur plus proche de l'adr. IP de destination. Message envoyé depuis le routeur par défaut qui corrige ainsi le routage
    - **Echo/réponse d'écho** teste la présence d'une machine sur le réseau
    - **Demande de réponse: d'estampille de temps:** échantillonne le temps AR entre deux équipements du réseau
    - **Demande et réponse d'informations** (périmé pour la recherche d'un réseau local)
    - **Demande et réponse de masque de sous réseau**
      - **pour déterminer le masque de sous réseau associé au réseau IP local**
  - **Une description plus élaborée est présentée dans l'un des chapîtres suivants**



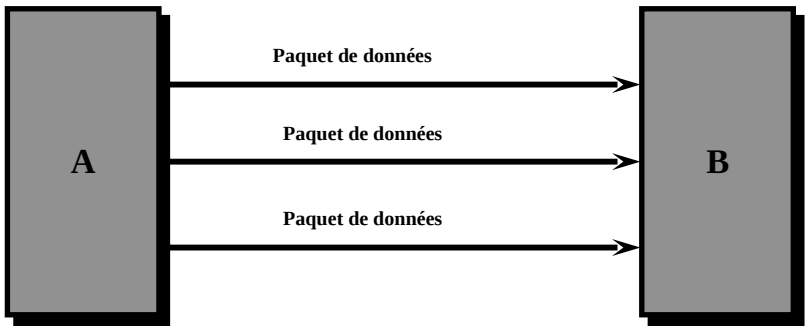
- **ARP SYNTHESE**
  - ➔ **Une description plus élaborée est présentée dans l'un des chapîtres suivants**



- **RFC Request For Comment**
  - **Décrivent une particularité de TCP/IP**
    - **utilisent des champs non occupés dans la trame**
      - **services**
      - **modification du noyau**
      - **etc....**
- **Etape 1**
  - **Discussions sur le réseau avec prises en compte de remarques d'origines informelles ou formelles lors de réunions de groupes de travail IETF**
- **Etape 2**
  - **Création du draft et distribution (récapitulatif de tous les commentaires générés par le RFC**
- **Etape 3**
  - **Proposition de standard (gestation durant 6 mois). Deux implémentations indépendantes et intéropérables devront être écrites et testées. Résolution des problèmes constatés**
- **Etape 4**
  - **Ecriture du Draft standard et attente durant 4 mois (autres implémentations en cours de tests)**
- **Etape 5**
  - **Adoption du standard**

UNIVERSITE D'EVRY
VAL D'ESSONNE

PRINCIPES



F 1.2NT: Exemple de communication sans connexion

10

- Différences entre service sur connexion et datagramme
  - Service sans connexion

➔ **Pas d'ouverture de connexion:**

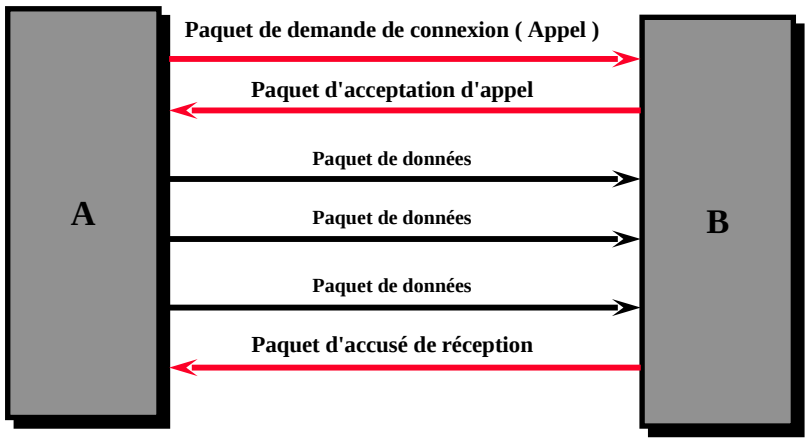
➔ **Transfert direct**

– **Pas de fermeture**

•se compare au courrier postal standard

UNIVERSITE D'EVRY
VAL D'ESSONNE

PRINCIPES



F 1.3 NT: Exemple de communication orientée connexion

- Différences entre service sur connexion et datagramme
  - service sur connexion

➔ **Pendant l'ouverture de connexion:**
  - **Réservation de ressources préalablement à la phase transfert**
  - **Choix d'un chemin pour ce transfert**

➔ **Pendant le transfert:**
  - **Respect du chemin choisi**
  - **Respect du séquencement d'origine à la livraison**
  - **Détection et corrections d'erreurs**
  - **Contrôle de flux entre Emetteur et Récepteur**

➔ **Après la fermeture**
  - **Libération totale des ressources**

•se compare : à une communication téléphonique

UNIVERSITE D'EVRY
VAL D'ESSONNE

Tables ARP

	INDEX IF	Adresse Physique	Adresse IP	Type
Entrée 1				
Entrée 2				
Entrée 3				
Entrée N				

Index IF:
le port (interface) physique
Adresse physique:
celle du composant
Adresse IP:
adresse IP correspondant à l'adresse physique
Type:
type d'entrée dans l'antémémoire ARP

- 1 aucun état
- 2 entrée invalide
- 3 mappage dynamique (permis)
- 4 mappage statique

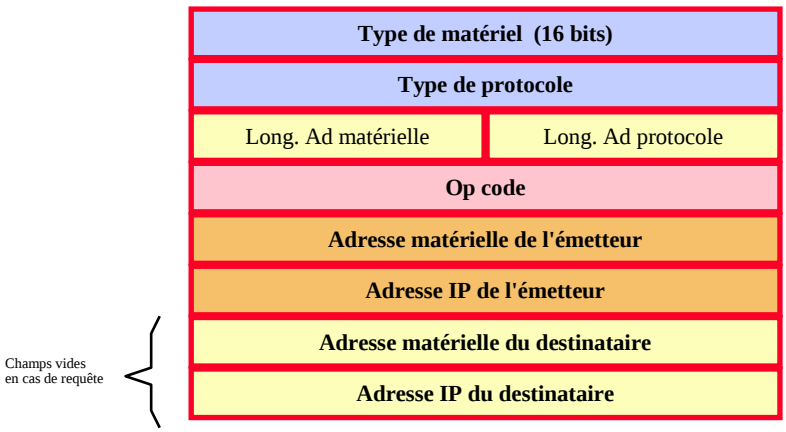
Table de conversion ARP

12

- **TABLE DE CONVERSION**
  - **On appelle cette table un cache ARP. Chaque ligne correspond à un composant.**
- **TYPE DE MAPPAGE (Type)**
  - **Quatre valeurs sont possibles (voir tableau)**
    - **Si ARP reçoit une adresse IP d'une machine de destination, il recherche une correspondance dans son cache.**
      - **s'il la trouve il renvoie l'adresse physique correspondante.**
      - **dans le cas contraire il envoie un message de broadcast (Requête ARP) contenant l'adresse IP du composant destinataire.**
      - **si une machine connaît l'adresse physique correspondante, elle la renvoie, l'initiateur met alors sa table à jour pour de futurs usages.**
      - **si l'adresse physique du destinataire n'est pas connue ou en l'absence de serveur d'adresses, la requête comporte un champ vide (Ad matérielle du destinataire) qui devra être complétée lors de la réponse (Voir diapo suivante)**
    - **Sur réception d'une requête par le cache, les informations qu'elle contient servent à la mise à jour de sa table. (les ajouts et modifications sont donc enregistrées au fil de l'eau).ARP**
    - **En conclusion un tel mécanisme protège la bande passante des sur-trafics.**

UNIVERSITE D'EVRY
VAL D'ESSONNE

ARP Formats de messages



Agencement des Requêtes et Réponses ARP

13

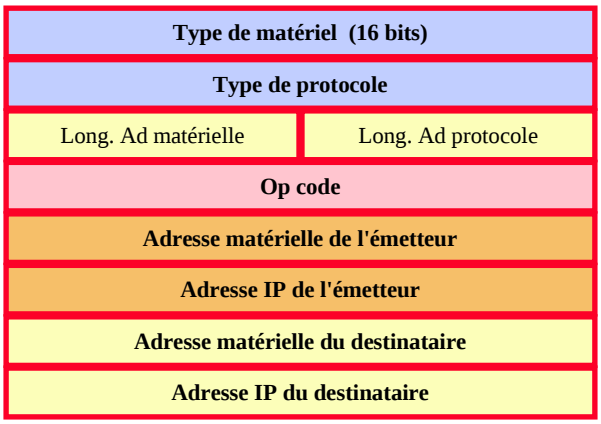
- **Requêtes et réponses ARP**
  - **Lorsqu'une requête ARP est envoyée tous les champs sont utilisés, sauf l'adresse matérielle du destinataire (celle que la requête souhaite identifier).**
  - **Dans une réponse tous les champs sont utilisés.**

➔ **formation de la trame (PDU)**

- **Ils sont agencés pour former une trame en les combinant avec les protocoles du système de réseau, les champs ont la signification suivante:**
  - **Hardware type: le type de l'interface matérielle.**
  - **Protocol type: le type de protocole utilisé par le composant émetteur.**
  - **Hardware Address Length: longueur en octet de chaque adresse matérielle dans le datagramme.**
  - **Protocol Address Length: longueur en octet de l'adresse du protocole dans le datagramme.**
  - **Opcode Opération Code: indique si le datagramme est une requête ARP (val=1) ou une réponse ARP (val=2)**
  - **Sender Hardw. Address: adresse matérielle du composant émetteur.**
  - **Sender IP Address: adresse IP du composant émetteur**
  - **Recipient IP Address: adresse IP du composant récepteur**
  - **Recipient Hardw. Address: adresse matérielle du composant récepteur**
- **Le détail du contenu est fourni ci-après.**

UNIVERSITE D'EVRY
VAL D'ESSONNE

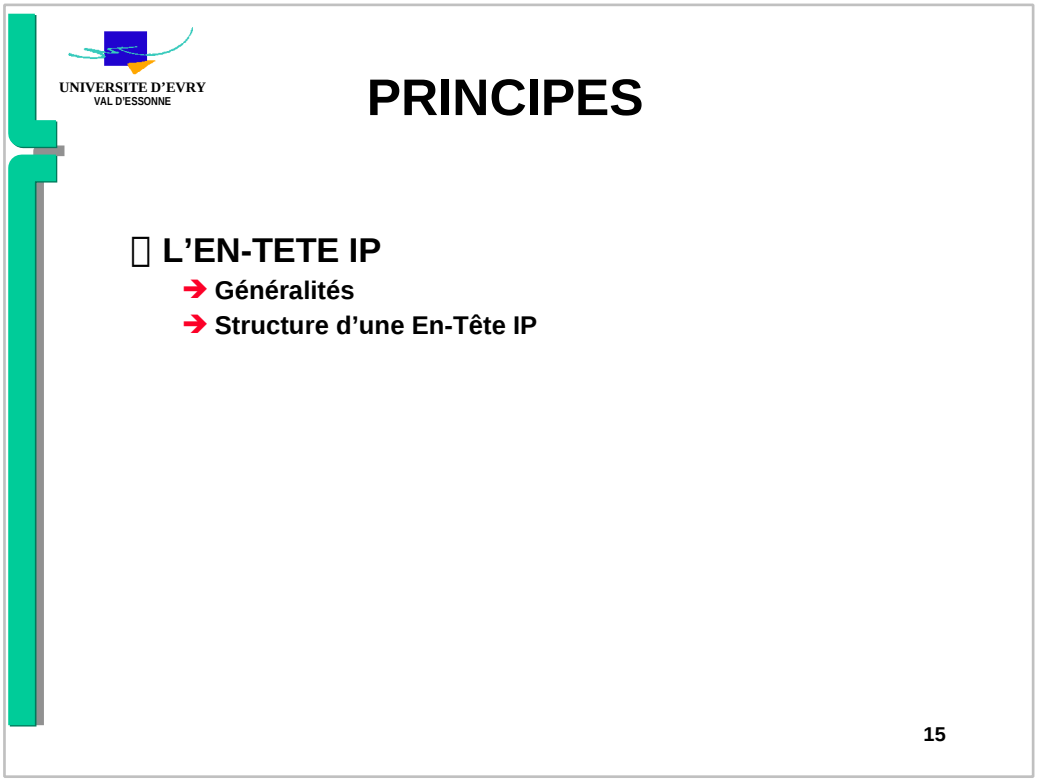
ARP Formats de messages



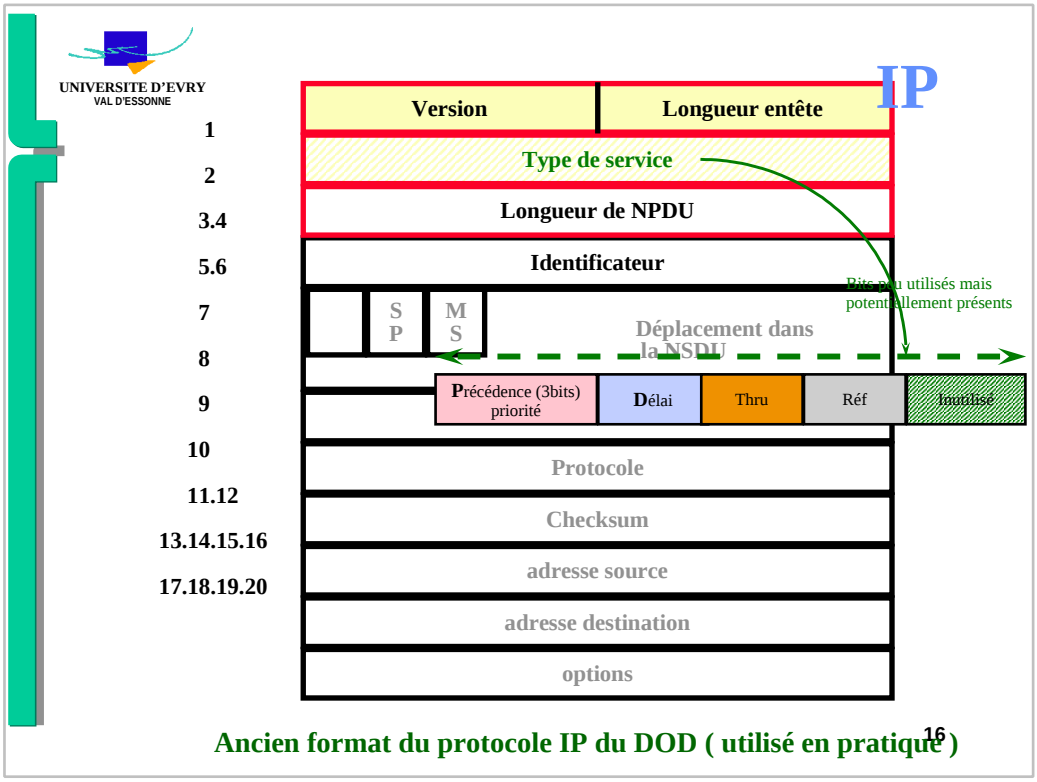
Requêtes et Réponses ARP - Contenus

14

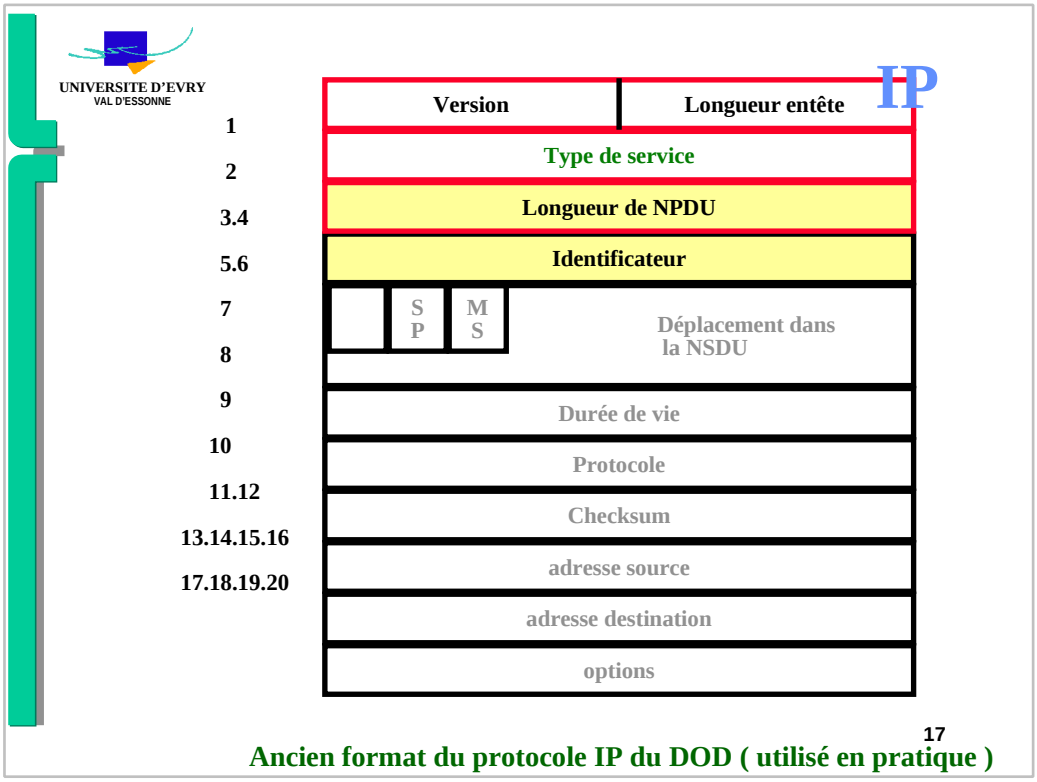
- **Contenu des des champs Types**
  - **Champs Type de Matériel (Valeurs)**
    - **1 Ethernet**
    - **2 Experimental Ethernet**
    - **3 X25**
    - **4 Proteon ProNET (Token Ring)**
    - **5 Chaos**
    - **6 802.X**
    - **7 Arcnet**
- **Le champ Type de protocole**
    - **512 XEROX PUP**
    - **513 PUP XEROX Translation**
    - **1536 XEROX NS IDP**
    - **2048 IP**
    - **2053 X25 niv 3**
    - **2054 ARP**
    - **2055 XNS**
    - **32821 RARP**
    - **32823 AppleTalk**
  - **etc.**



- **En-tête IP Généralités**
  - **Le datagramme est l'unité de transfert IP.**
  - **Les spécifications d'IP et autres protocoles de la famille TCP/IP définissent les en-tête et les queues (trailer) en termes de mots. Un mot représentant 32 bits en V4.**
  - **L'en-tête IP est donc composée de six mots ou 24 Octets, tous les champs facultatifs y sont inclus.**



- **STRUCTURE D'UNE ENTETE IP:**
  - **Oct 1**
    - **Version**
      - **Format d'entête utilisé (plusieurs format existent) composition sur 4 bits.**
    - **Longueur Entête**
      - **Indiquée en multiple de mots de 4 octets,**
      - **5 mots par défaut (20 octets),**
      - **6 mots maxi (24 octets) avec les champs facultatifs.**
        - **elle est utilisée pour calculer un décalage et savoir par déduction ou commencent les données.**
  - **Oct 2**
    - **TOS (Type de Service): Utilisé par les passerelles pour sélectionner les paramètres de transmission réels d'un sous réseau donné.**
      - **3 bits P = priorité 8 niveaux de priorité d'acheminement (low=000)**
      - **1 bit D = Délai _ 1 bit T= Débit _ 1 bit R= fiabilité (low=0 high=1)**
      - **2 bits à 0 réservés**
      - **Le TOS est important car il entraîne dans tous les cas ou cela est possible une violation des restrictions de contrôle de flux. (Urg)**
      - **Ils décrivent la qualité de service désirée, soit favoriser:**
        - **le délai de transmission, le débit, la sûreté de transmission**



- **STRUCTURE D'UNE ENTETE IP:**
  - **Oct 3,4**
    - **Longueur NPDU (ou du Datagramme)**
      - **En nombre d'octets, en-tête compris.**
        - **la longueur de la zone de donnée peut être calculée en soustrayant de cette valeur la longueur de l'En-tête.**
      - **La taille maximale du datagramme est de 65535 octets.**
  - **Oct 5,6**
    - **Identificateur (Unique)**
      - **Pour reconnaître les différents fragments du segment initial.**
        - **il est nécessaire pour reconstruire le message initial fragmenté lors du réassemblage.**
      - **Attribué par l'émetteur à chaque segment. (modulo 2^{32})**
        - **chacun des datagrammes fragmentés possède le même N° d'identification ce qui permet de ne pas les confondre avec les fragments d'un autre message.**

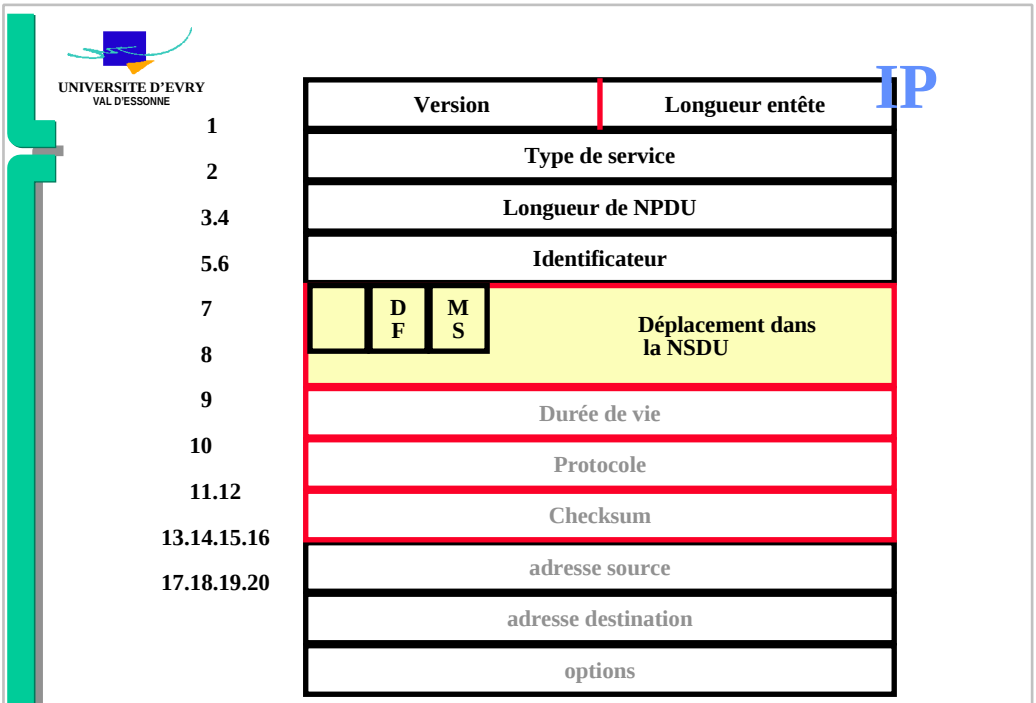


Fig 6.14 : Ancien format du protocole IP du DOD (utilisé en pratique)

- **STRUCTURE D'UNE ENTETE IP suite :**
  - **Oct 7,8**
    - **Flags (Champ à 3 bits dont un inutilisé)**
      - **DF -Don't Fragment: si val = 1 n'autorise pas la fragmentation**
      - **MS -More Segment : si val = 1 positionné indique que ce n'est pas le dernier fragment dans le segment initial,**
      - **Le dernier fragment aura ce flag positionné à val = 0, le composant récepteur cessera d'attendre des segments.**
      - **L'ordre d'arrivée étant aléatoire MF sera utilisé avec le décalage fragment pour indiquer au récepteur la forme du message complet.**
    - **Déplacement (décalage fragment) 13 bits**
      - **Si MF est à 1 (message fragmenté) il indique la position du fragment dans le segment original à réassembler.**
      - **les décalages sont calculés par rapport au début du message en unités de 8 octets (correspondants à la longueur maximale de message: 65535 octets).**
      - **IP récepteur l'utilise pour réassembler en observant également l'unicité de celui-ci grâce à l'Identificateur.**

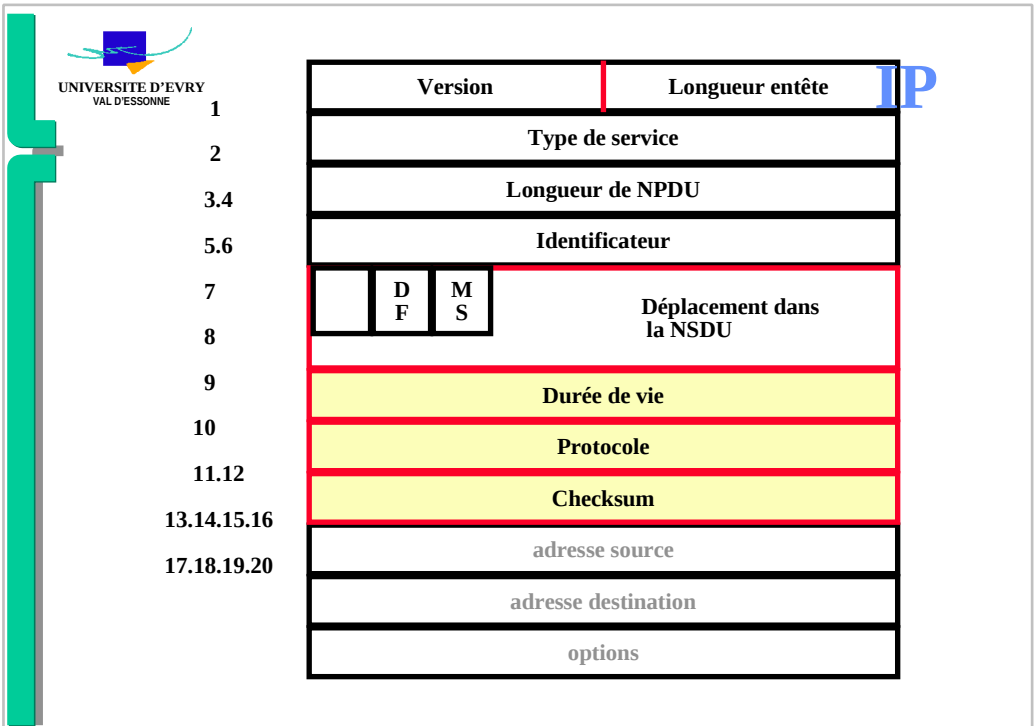


Fig 6.14 : Ancien format du protocole IP du DOD (utilisé en pratique)

- Oct 9
  - Durée de Vie (Protection de la bande passante)
    - Borne supérieure de temps de vie du segment affecté par l'émetteur et décrémenté par les routeurs.
    - Si fragmentation, chaque fragment reçoit la durée de vie courante du fragment ou segment sur lequel est appliquée cette fragmentation.
    - Val: 15 ou 30 secondes et décémentation d'1 sec par noeud traitant le datagramme
      - à l'arrivée dans une passerelle le temps d'arrivée est noté, le temps d'attente dans une passerelle surchargée va avoir un effet désastreux sur la durée de vie. du datagramme; le TTL expirant alors que celui-ci est en attente de traitement. Un message est alors renvoyé à la machine origine qui le répétera.
- Oct 10
  - Protocole
    - Indique le N° d'identification du protocole de niveau supérieur devant recevoir le datagramme
      - ces protocoles sont définis par le NIC; 50 protocoles sont ainsi référencés, les plus important sont TCP (6) et ICMP (1).
- Oct 11,12
  - Checksum
    - Somme de contrôle de l'entête, le TTL étant décrémenté à chaque noeud entraîne le recalcule du FCS

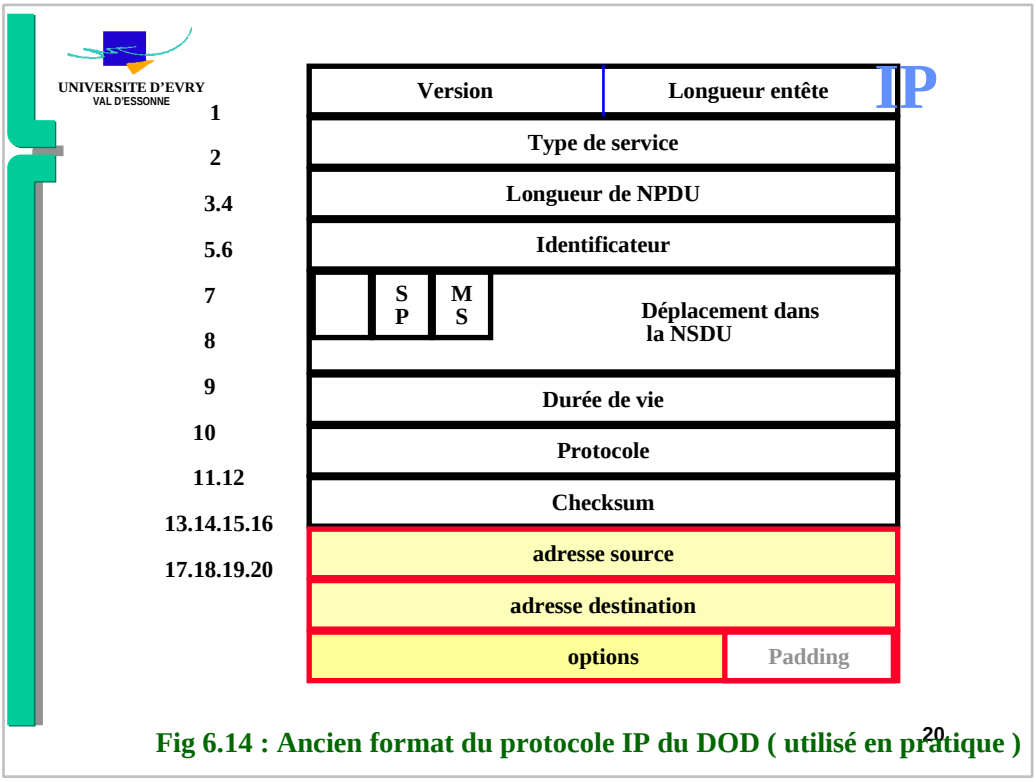


Fig 6.14 : Ancien format du protocole IP du DOD (utilisé en pratique)

20

❒ **STRUCTURE D'UNE ENTETE IP suite :**

- ➔ **Oct 13-16 Adr. Source**
- ➔ **Oct 17-20 Adr. Destinataire**
  - ◆ **-Sur 4 Oct = longueur fixe, les sous-adressages privés sont plus complexes à créer**
    - ♦ **Une instance internationale règle ce type de problème pour les grands réseaux**
- ➔ **n Oct = Options (champs optionnels de longueur variable)**
  - ◆ **Il est composé de codes à longueur variable.**
  - ◆ **Si plus d'une est utilisée dans le datagramme, elles apparaissent à la suite les unes des autres.**
    - ♦ **Toutes les options sont contrôlées par un octet, généralement divisé en trois champs:**
    - ♦ **Flag de copie (1 bit) si fragmentation dans une passerelle:**
      - **val = 0 option copiée sur le datagramme mais pas sur les suivants**
      - **val =1 option copiée sur tous les datagrammes**
    - ♦ **Classe d'option (2 bits)**
      - **voir tableau suivant**
    - ♦ **N° d'option (5 bits)**
      - **voir tableau suivant**

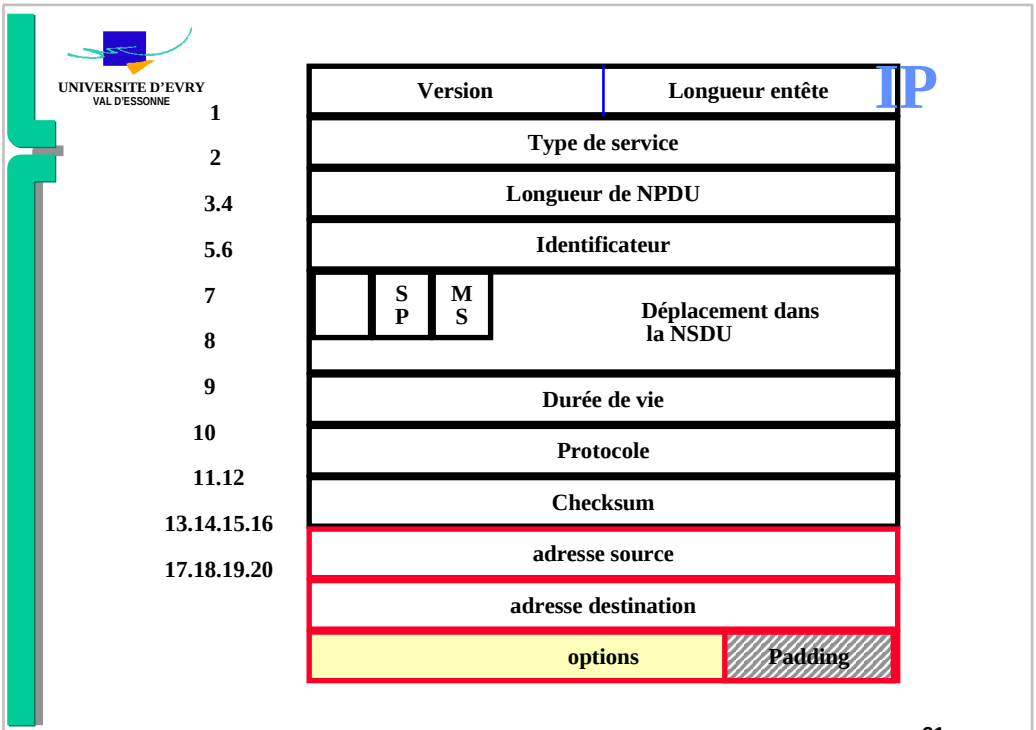


Fig 6.14 : Ancien format du protocole IP du DOD (utilisé en pratique)

- **STRUCTURE D'UNE ENTETE IP suite :**
  - **Oct = var Options**

Classe	N°	Description
0	0	Fin de liste d'option
0	1	Aucune option (remplissage)
0	2	Option de sécurité (Militaire)
0	3	Routage tolérant (Loose routing)
0	7	Active l'enregistrement du routage ajout de champs (utile au diagnostics)
0	9	Routage strict (IP ad de passerelles imposées)
2	4	Marquage de date activé (Ajout de champs) en TU

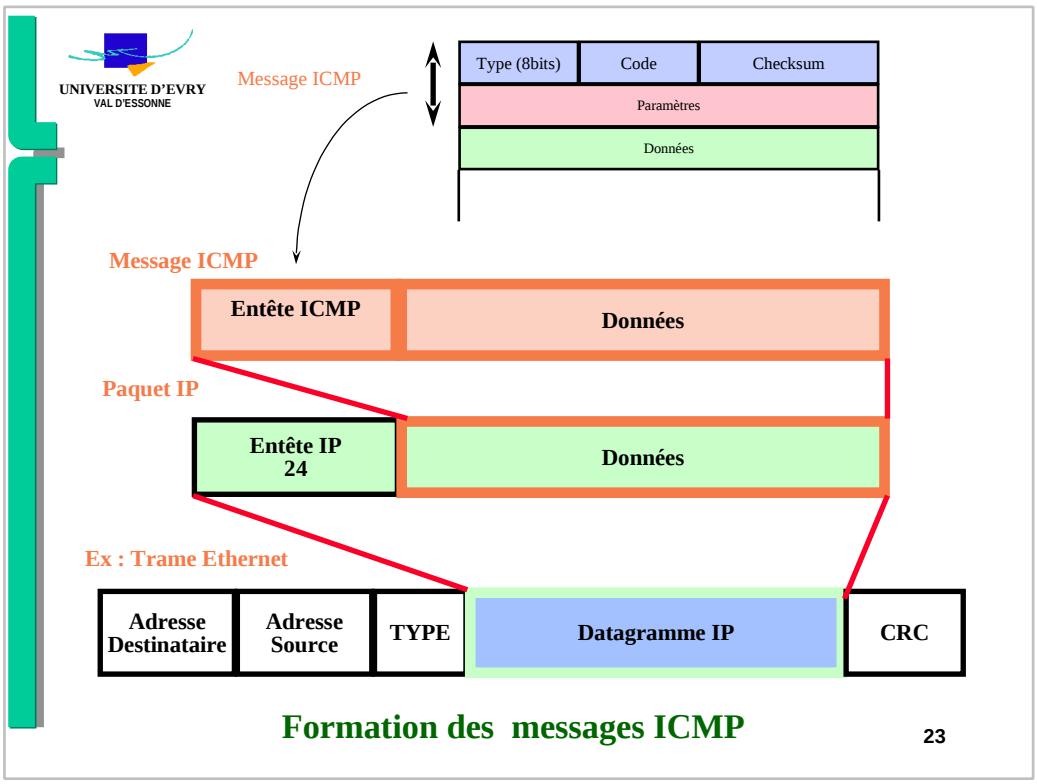
  - **les options 7 et 4 permettent de tracer le datagramme au passage dans l'inter-réseau.**
  - **attention au format du timestamp exprimé en millisecs après minuit en TU. le système d'horloge peut être problématique même si étalonné en TU.**
  - **l'options 3 fournit une série d'adresses par où le datagramme doit passer, mais ne bloque pas le parcours intermédiaire qui reste libre.**
  - **l'option 9 n'autorise aucune déviation de bout en bout, si le parcours est impossible le datagramme est abandonné. Utilisé surtout pour tester les routes, rarement en exploitation.**
  - **Padding** **Garantie d'une long. d'en-tête en octets entière**

UNIVERSITE D'EVRY
VAL D'ESSONNE

PRINCIPES

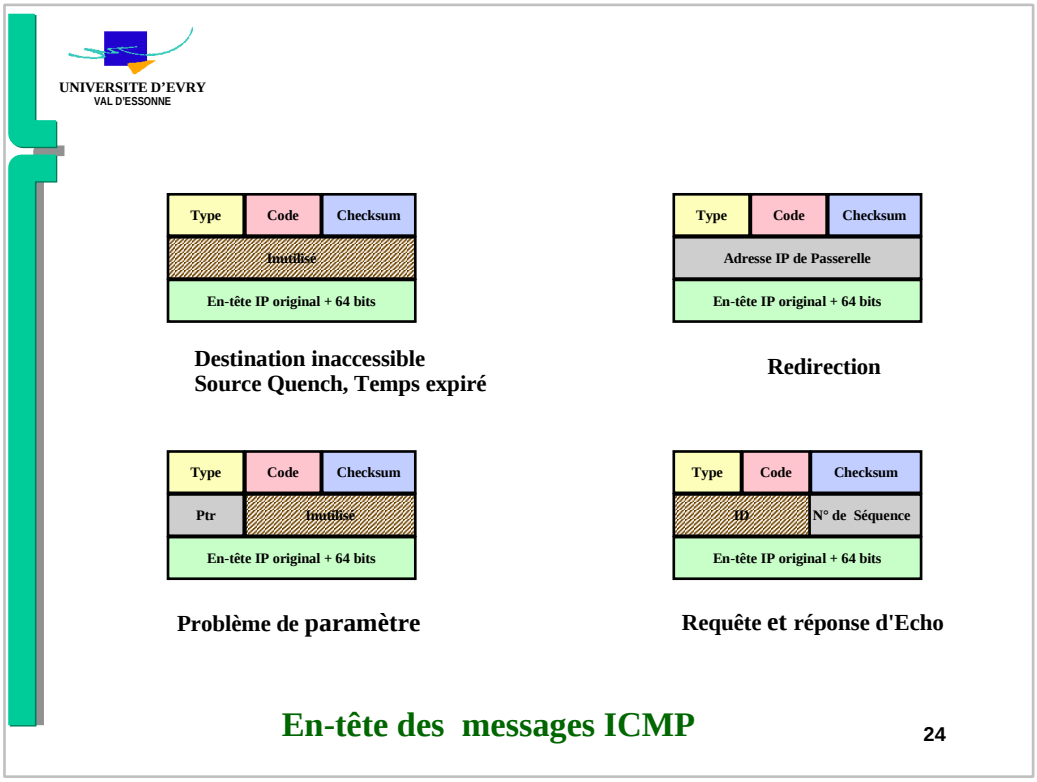
- **MESSAGES ICMP**
  - ➔**Système de rapport d'erreur IP**
  - ➔**Formats des En-Têtes ICMP**
  - ➔**Agencements selon les types de messages**

22

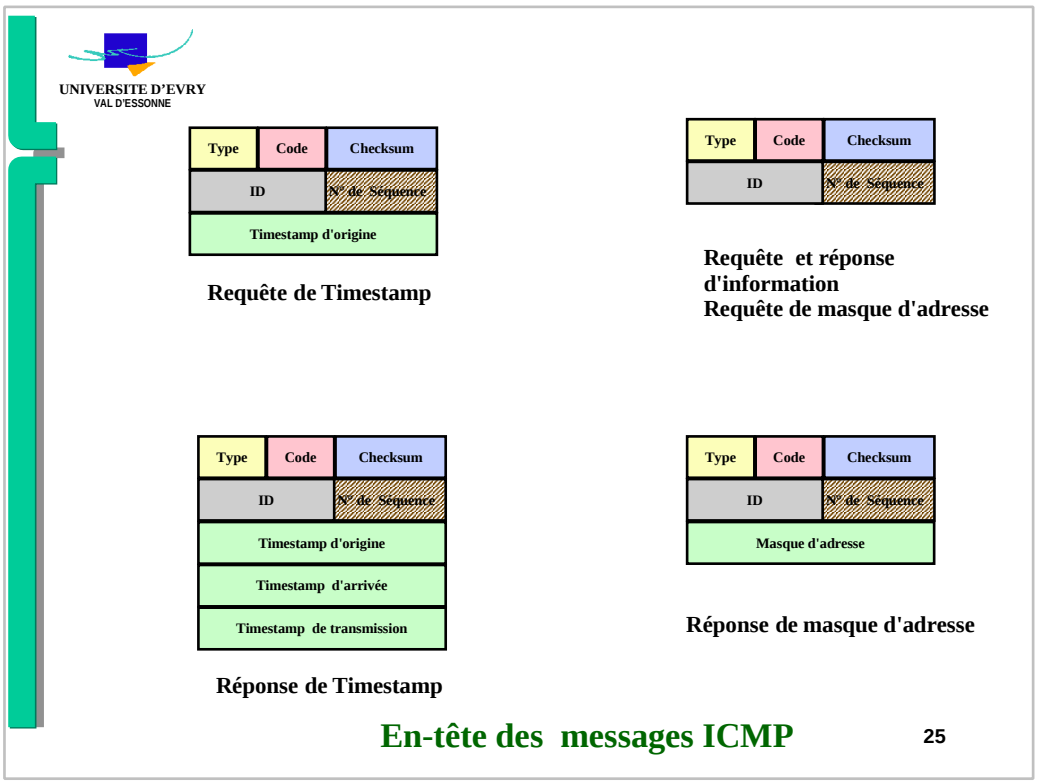


- **ICMP Système de rapport d'erreur d'IP**
  - **Traité par la couche réseau comme n'importe quel datagramme, mais interprétés spécifiquement par IP**
    - **ces messages sont retournés à la machine émettrice du datagramme posant problème**
    - **il permettent à l'émetteur de décider la meilleure manière de renvoyer le datagramme en fonction du message fourni par ICMP**
- **Formats ICMP**
  - **Valeurs valides pour le champ Type**

Valeur	Description
0	Echo reply
3	Destination inaccessible
4	Source quench
5	Redirection
8	Demande d'écho
11	TTL expiré
12	Problème de paramètre
13	Requête de timestamp
14	Réponse de timestamp
15	Requête d'information obsolète
16	Réponse d'information obsolète
17	Requête de masque d'adresse
18	Réponse de masque d'adresse



- ICMP
  - Champs Code et Cheksum
    - Il précise le type de message, calcul identique à l'en-tête pour le checksum.
  - Agencements selon les type de messages
    - Destination non accessible et TTL expiré
      - ils sont aussi utilisés lorsqu'un datagramme doit être fragmenté alors que le flag DF est activé: *un message Dest. non atteignable est envoyé*
    - Source Quench
      - contrôle de flux élémentaire, origine gateway ou hôte saturé ou ayant atteint un taux de remplissage de buffers donné.
        - sur réception le destinataire doit réduire le taux de transmission sur le réseau jusqu'à cessation des Source Quench.
        - chaque datagramme ignoré entraîne l'émission d'un Source Quench
    - Redirection
      - Envoyés à la passerelle du chemin pour indiquer une meilleure route.
        - le message provenant d'une autre passerelle arrive. La passerelle réceptrice regarde les données, mais connaît une meilleure route.
        - elle informe l'expéditrice de l'adresse IP de cette route et un entier est placé dans le champ de code de l'en-tête, valeurs:
        - 0 - les datagr. destinés à tous composants du réseau seront redirigés
        - 1 - seuls ceux destinés au composant précisé seront redirigés
        - 2 - les datagr. à destin. du réseau ayant le même type de service (voir en-tête) seront redirigés
        - 3 - redirection des datagr. à même type de service et destiné au même hôte



- **ICMP**
  - **Agencements selon les types de messages**
    - **Problème de paramètre**
      - **message envoyé si une erreur syntaxique ou sémantique est rencontrée dans l'en-tête IP, ex: arguments non valides dans une option, l'octet cause du problème est ciblé par un pointeur (Ptr).**
    - **Requête et réponse d'écho (ex: Ping)**
      - **messages souvent utilisés en débogage. Si une requête est envoyée, un composant ou une passerelle situé en aval du chemin renvoie une réponse au composant spécifié. Ceci permet en autres:**
      - **d'identifier des problèmes de reroutage**
      - **des dysfonctionnement de passerelle**
      - **des problèmes de câblages**
    - **Requête et réponse Timestamp**
      - **elles permettent de chronométrer les passages du message dans le réseau**
      - **combinée à des options de routages strictes elles permettent de mettre en évidence les goulots d'étranglement**
    - **Requête et réponse de masque d'adresse**
      - **elles sont utilisées à des fins de test, au sein d'un réseau ou sous réseau spécifique**