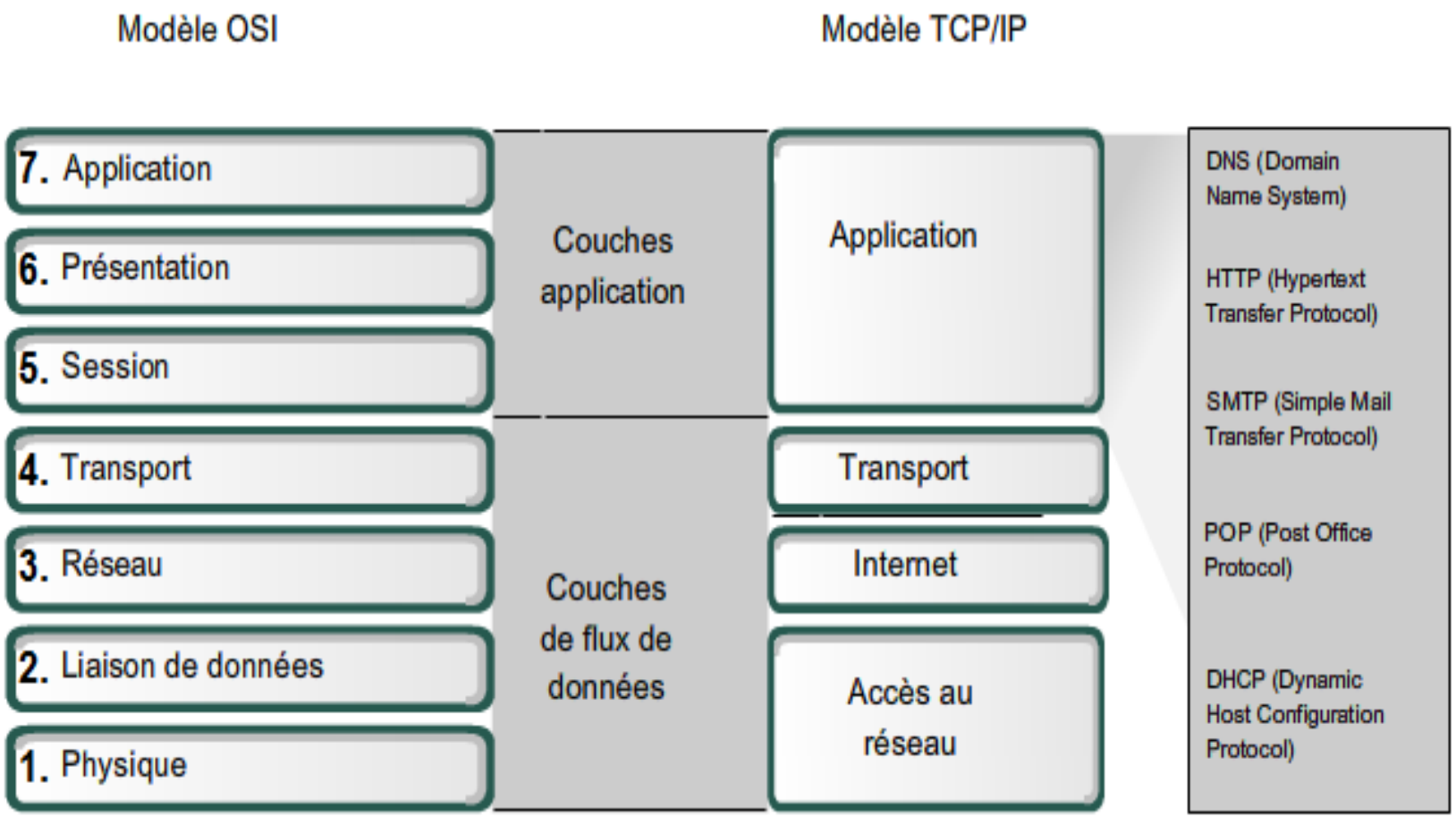
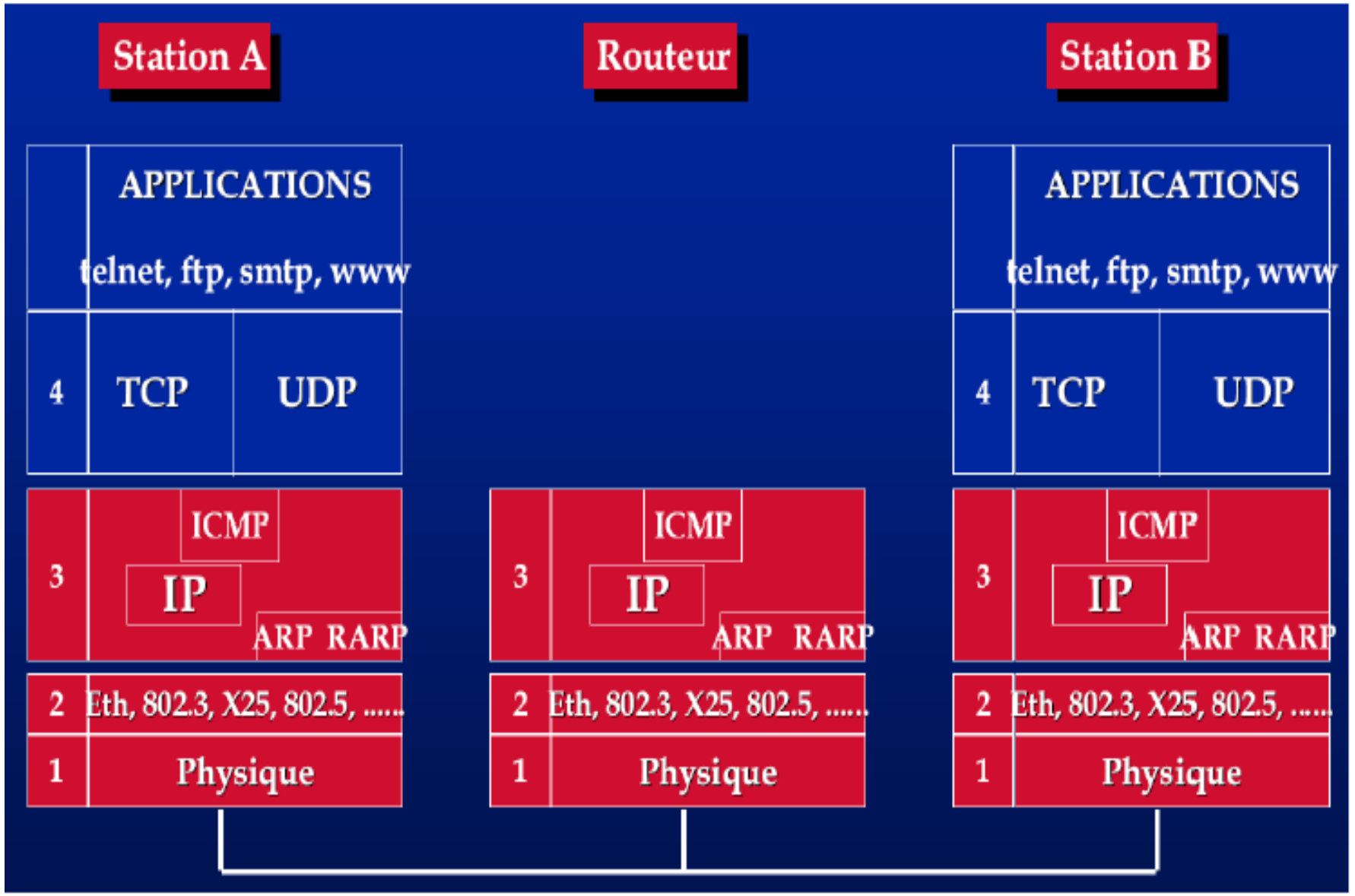
Couche réseau

Fondements des réseaux

TCP/IP Vs OSI


Modèle OSI
Modèle TCP/IP
7. Application
6. Présentation
5. Session
4. Transport
3. Réseau
2. Liaison de données
1. Physique
Couches application
Couches de flux de données
Application
Transport
Internet
Accès au réseau
DNS (Domain Name System)
HTTP (Hypertext Transfer Protocol)
SMTP (Simple Mail Transfer Protocol)
POP (Post Office Protocol)
DHCP (Dynamic Host Configuration Protocol)

Modèle en couche



La couche réseau

- La couche réseau (couche 3 OSI) fournit des services pour l'échange des éléments de données sur le réseau entre des périphériques finaux. Pour effectuer ce transport de bout en bout, la couche 3 utilise quatre processus de base :
  1. l'adressage logique
  2. l'encapsulation
  3. le routage
  4. la décapsulation

Couche Internet

- IP
- ICMP
- ARP
- RARP

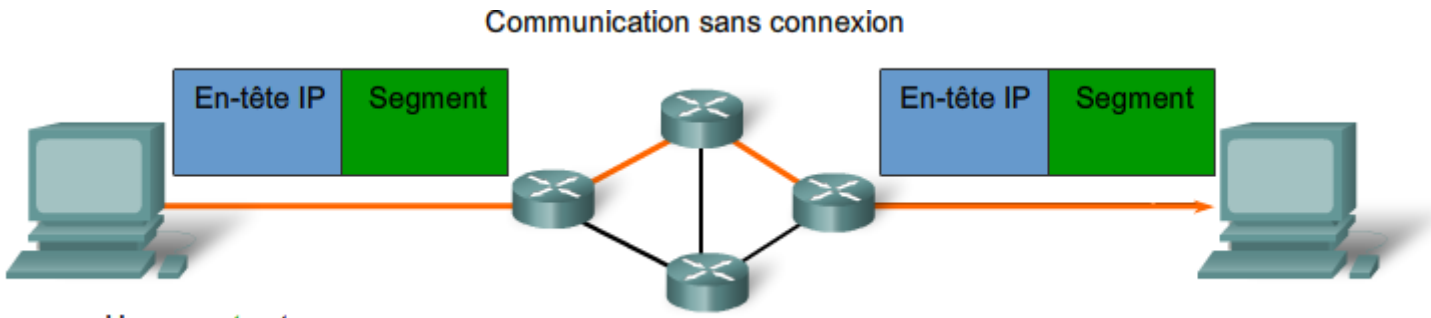
Le protocole IP

- Le protocole de la couche réseau le plus répondu est le protocole IP (*)
- IP pour « Internet Protocol » est utilisé pour transporter des données utilisateur sur le réseau
- IP v4 a pour caractéristiques:
  - ✓ Sans Connexion: aucune connexion n'est établie avant l'envoi de paquets de données.
  - ✓ Au mieux (peu fiable) : aucune surcharge n'est utilisée pour garantir la transmission des paquets.
  - ✓ Indépendant du média transportant les données.

(*) CCNA R&S (v6.0)

Le protocole IP

- Sans connexion:



L'expéditeur ne sait pas :

- si le destinataire est présent
- si le paquet est arrivé
- si le destinataire peut lire le paquet

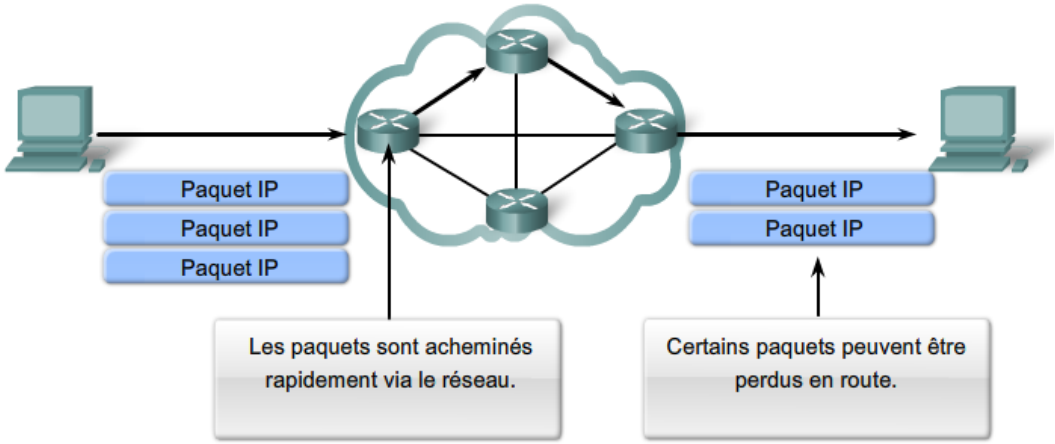
Le destinataire ne sait pas :

- quand il arrive

Le protocole IP

- Service au mieux:

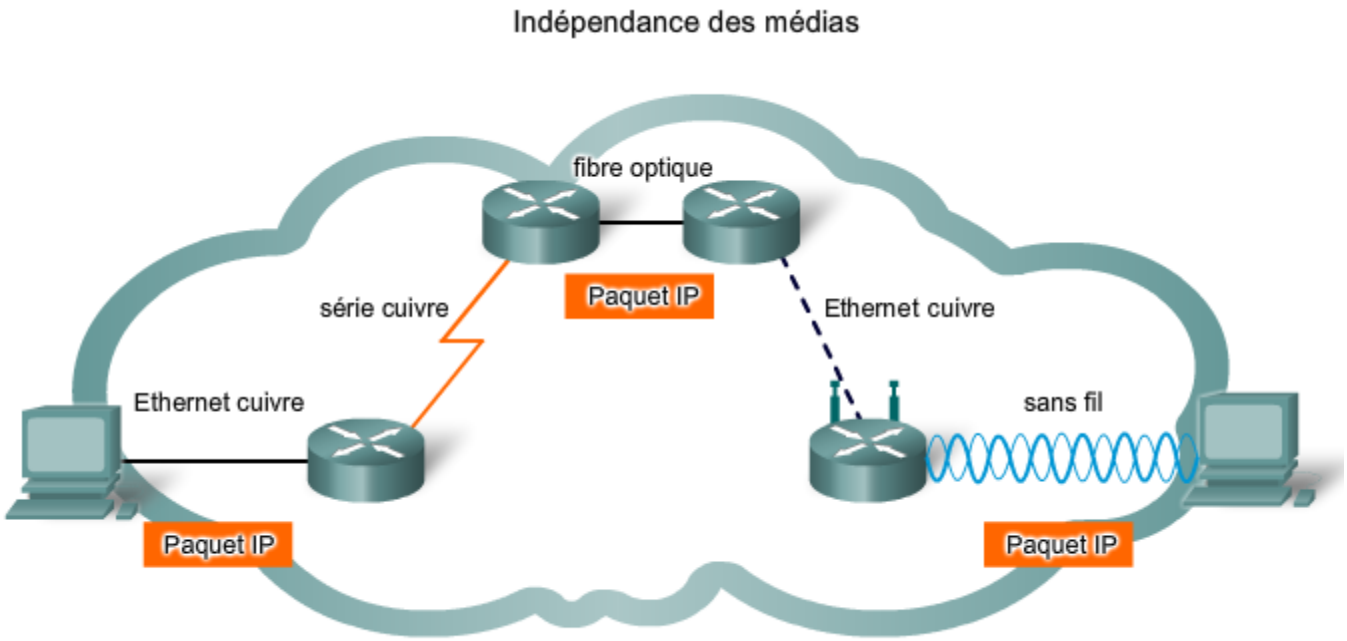
  Peu fiable signifie simplement que le protocole IP n'a pas l
  capacité de gérer ni de récupérer des paquets non délivrés ou
  corrompus.



Protocole de couche réseau peu fiable, IP ne garantit pas que tous les paquets envoyés seront reçus.

Le protocole IP

- Indépendant de média:



Les paquets IP peuvent transiter par différents médias.

Le protocole IP

- La couche réseau tient compte, cependant, d'une caractéristique majeure : la taille maximale d'unité de données de protocole que chaque média peut transporter. Cette caractéristique est désignée comme unité de transmission maximale (MTU).
- Dans certains cas, un périphérique intermédiaire (généralement, un routeur) devra scinder un paquet lors de sa transmission d'un média à un autre avec une MTU inférieure. Ce processus est appelé fragmentation du paquet.

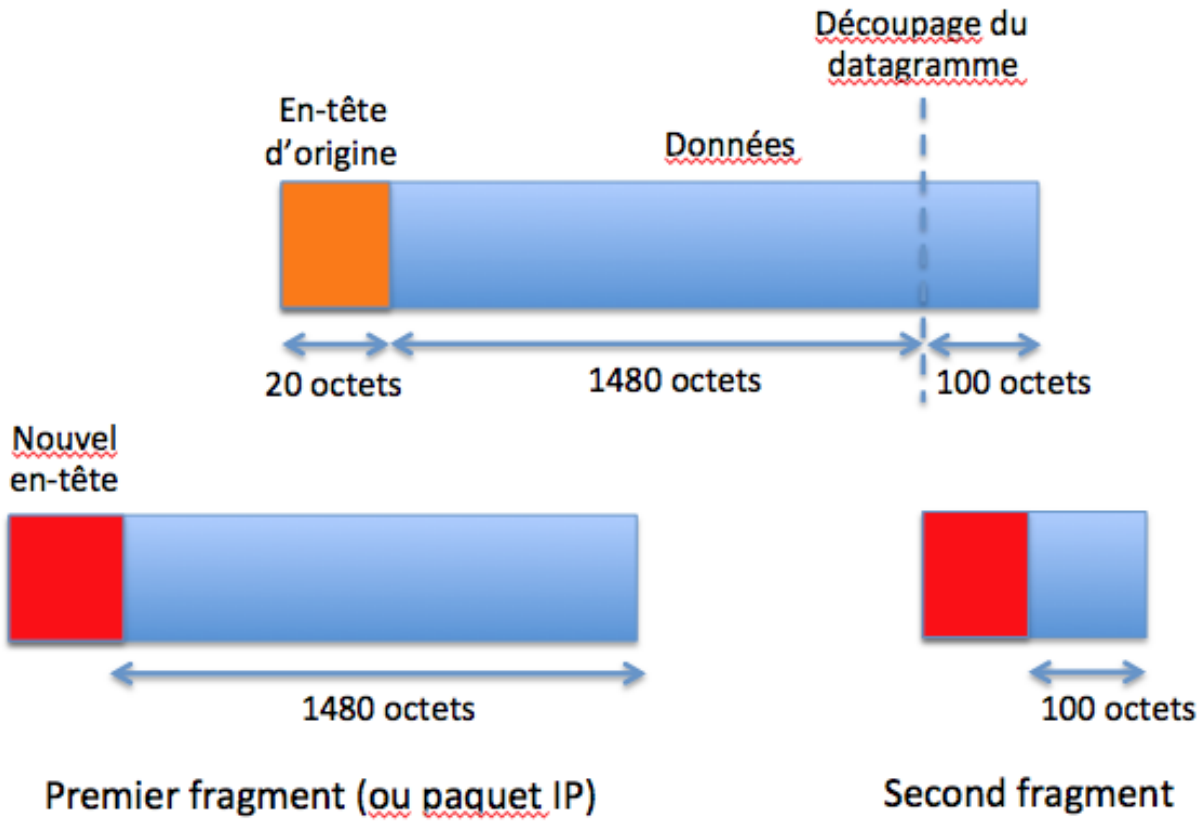
La fragmentation

- La fragmentation va donc être un rôle secondaire de la couche 3 qui devra permettre de découper un datagramme en plusieurs paquets ET de reconstituer ces paquets à la machine destinatrice.
- La difficulté va donc être de pouvoir découper, puis recomposer les paquets reçus, même s'ils ne prennent pas le même chemin et arrivent dans le désordre, ou alors que l'un d'entre eux est perdu.

La fragmentation

- Exemple: Imaginons que notre machine souhaite envoyer un datagramme de 1600 octets. Une trame pouvant transporter un datagramme de 1500 octets -> il va falloir fragmenter ce datagramme
- Où va-t-on couper???? Au début? Au milieu? A la fin???

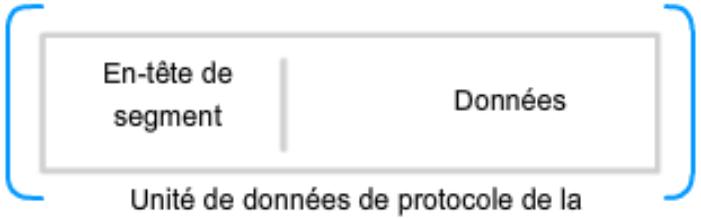
La fragmentation



Le protocole IP

Génération de paquet IP

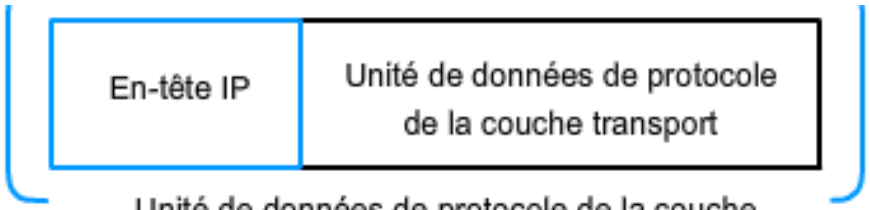
Encapsulation de la couche transport



Unité de données de protocole de la couche transport

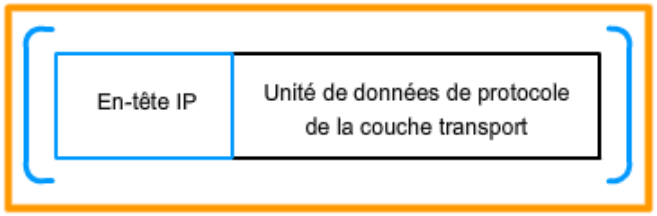
La couche transport ajoute un en-tête pour que les segments puissent être pris en compte et réordonnés à destination.

Encapsulation de la couche réseau



Unité de données de protocole de la couche réseau

La couche réseau ajoute un en-tête pour que les paquets puissent être acheminés via des réseaux complexes et atteignent leur destination.

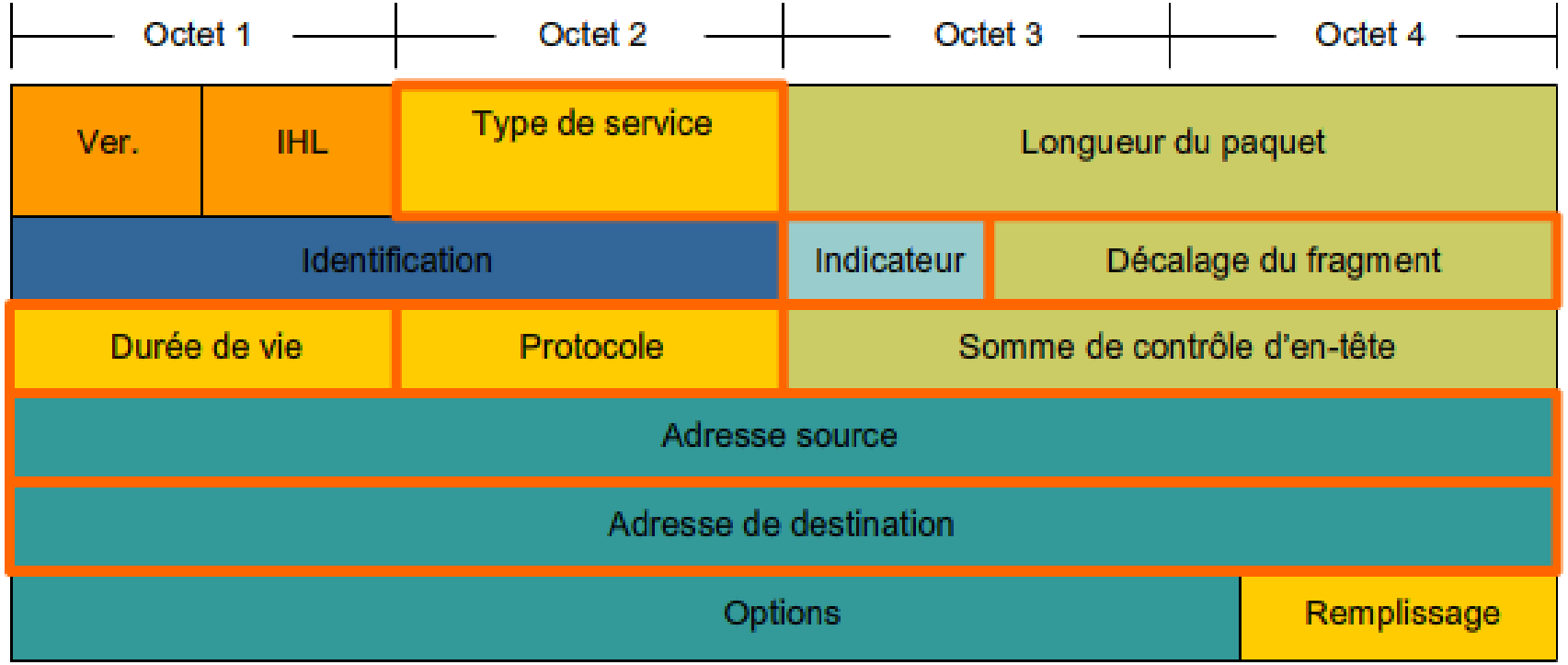


Paquet IP

DATAGRAMME IP

Entête IPv4

Entête IP: taille minimum 20 octets



Champs de l'entête IPv4

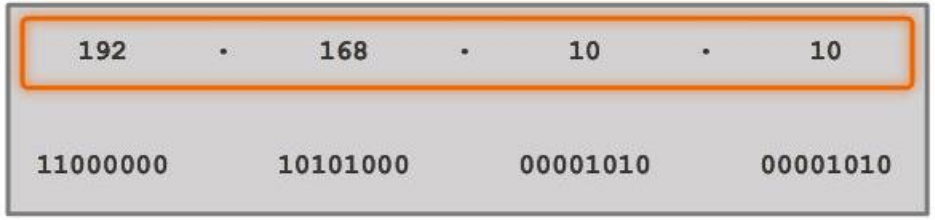
- **VERS** : numéro de version de protocole IP
- **IHL** : longueur de l'en-tête en mots de 32 bits, généralement égal à 5 (pas d'option),
- **Types de services:** ancien type de service codé sur 8 bits. Utilisé pour donner une priorité plus élevée que les autres à un paquet. Mais cela a été très peu utilisé.
- **Longueur totale** : longueur totale du datagramme en octets (en-tête + données)
- **Identification** – ce champ de 16 bits identifie de manière unique le fragment d'un paquet IP d'origine.
- **Indicateurs** – ce champ de 3 bits donne une information sur la fragmentation.
- **Décalage du fragment** – ce champ de 13 bits indique la position du fragment dans le paquet d'origine.

Champs de l'entête IPv4

- **Durée de vie** : codé sur 8 bits. Il est utilisé pour limiter la durée de vie d'un paquet. Les passerelles qui traitent le datagramme doivent décrémenter cette valeur de 1. Lorsque cette valeur atteint 0 (expire) le datagramme est détruit et un message d'erreur est renvoyé à l'émetteur.
- **Protocole**: Ce champ identifie le protocole de niveau supérieur véhiculé dans le champ données du datagramme : TCP:6, UDP:17, ICMP:1
- **Somme de contrôle de l'en-tête** : champ de 16 bits utilisé pour le contrôle des erreurs sur l'en-tête IP.
- **Adresse IP source** – contient une valeur binaire de 32 bits qui représente l'adresse IP source du paquet.
- **Adresse IP de destination** – contient une valeur binaire de 32 bits qui représente l'adresse IP de destination du paquet.

Format de l'adresse IPv4

- Une adresse IPv4 est codée sur 32 bits
- Elle est représentée en format décimal: 4 octets séparés de « . » : 192.168.10.10



192.168.10.10 est une adresse IP attribuée à un ordinateur.

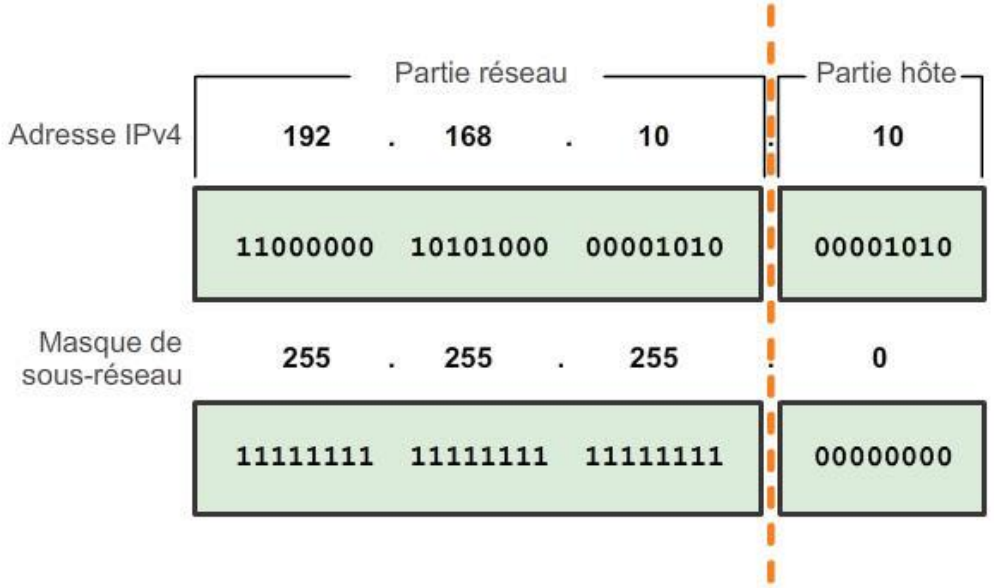
Base	2	2	2	2	2	2	2	2
Exposant	7	6	5	4	3	2	1	0
Valeurs des bits de l'octet	128	64	32	16	8	4	2	1
Adresse binaire	1	1	0	0	0	0	0	0
Valeurs binaires des bits	128	64	0	0	0	0	0	0

Ajouter les valeurs binaires des bits

128 + 64 = 192

Partie réseau et partie hôte d'adresse IPv4

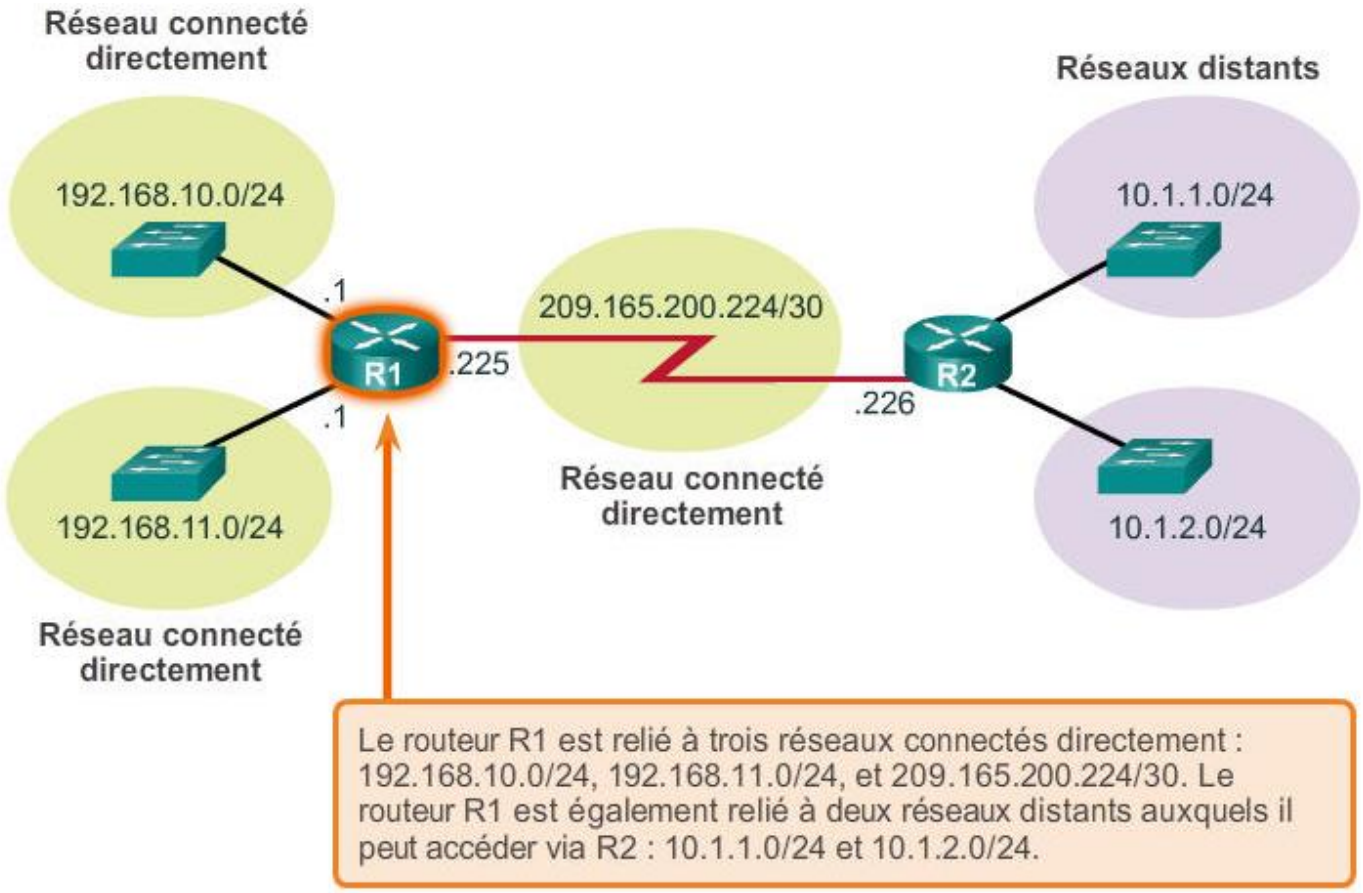
- Pour définir les parties réseau et hôte d'une adresse, les périphériques utilisent un modèle 32 bits distinct appelé masque de sous-réseau
- Le masque de sous-réseau ne contient pas réellement le réseau ou la partie hôte d'une adresse IPv4 ; il indique simplement où rechercher ces parties dans une adresse IPv4 donnée



Le routage

- Le rôle de la couche réseau est de diriger les paquets entre les hôtes (routage)
- Un hôte peut envoyer un paquet à lui-même, à un hôte local ou à un hôte distant
- Le fait que l'hôte destination est local ou distant est déterminé par la comparaison de l'adresse réseau destination avec celle source.
- Si l'hôte destination est distant (un autre réseau distinct de la source) alors l'aide du routeur et du routage est nécessaire.
- Le routage consiste à déterminer le meilleur chemin vers la destination.
- Les meilleurs chemins sont enregistrés dans une table appelée table de routage
- L'interface du routeur connectée au segment d'un réseau LAN est dite passerelle par défaut

Le routage

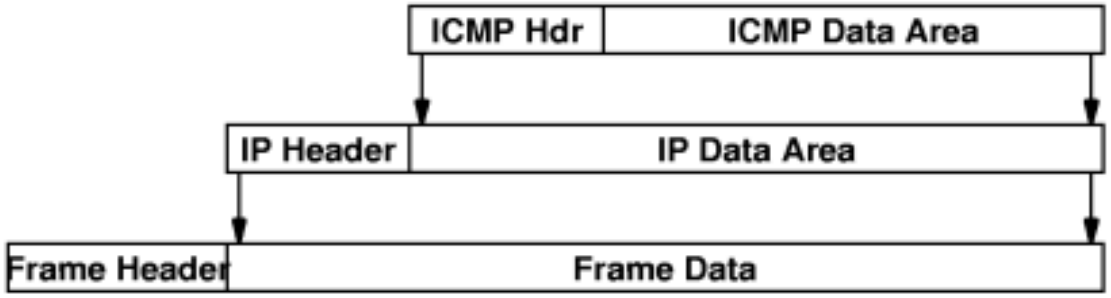

Réseau connecté directement
Réseaux distants
192.168.10.0/24
10.1.1.0/24
.1
209.165.200.224/30
R1
.225
R2
.226
.1
192.168.11.0/24
Réseau connecté directement
10.1.2.0/24
Réseau connecté directement
Le routeur R1 est relié à trois réseaux connectés directement : 192.168.10.0/24, 192.168.11.0/24, et 209.165.200.224/30. Le routeur R1 est également relié à deux réseaux distants auxquels il peut accéder via R2 : 10.1.1.0/24 et 10.1.2.0/24.

ICMP (Internet Control Message Protocol)rfc 792

- Le protocole ICMP (Internet Control Message Protocol) permet d'envoyer des messages de contrôle ou d'erreur vers d'autres machines ou passerelles.
- ICMP signale les erreurs à l'émetteur initial (il ne les corrige pas).
- Beaucoup d'erreurs sont causées par l'émetteur, mais d'autres sont dues à des problèmes d'interconnexions rencontrées sur l'Internet :
  - machine destination déconnectée,
  - durée de vie du datagramme expirée,
  - congestion de passerelles intermédiaires.
- Si une passerelle détecte un problème sur un datagramme IP, elle le détruit et émet un message ICMP pour informer l'émetteur initial.
- Les messages ICMP sont véhiculés à l'intérieur de datagrammes IP (protocole = 1) et sont routés comme n'importe quel datagramme IP sur l'Internet.
- Une erreur engendrée par un message ICMP ne peut donner naissance à un autre message ICMP (évite l'effet cumulatif).

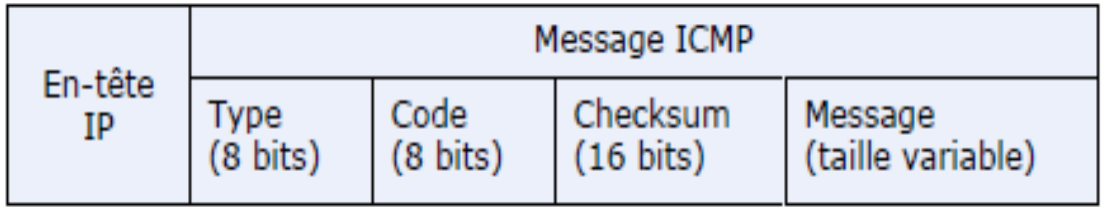
Encapsulation ICMP

- Message ICMP encapsulé dans un datagramme IP (champ **Protocole** de l'en-tête IP = 1)
- Paquet IP encapsulé dans une trame, pour être transmis



Format du message ICMP

- Message ICMP encapsulé par IP :



- Type (1 octet) : type de service ICMP
- Code (1 octet) : subdivision du type de service
- Total de contrôle (2 octets) : protection du contenu du message ICMP (même algorithme que IP)
- Autres champs (4 octets), selon la valeur du champ Type (numéro de séquence, identificateur, adresse IP…)
- Données ICMP :
  - Données (Echo), adresse IP, masque d'adresse, date...
  - En-tête IP et 8 premiers octets du datagramme en erreur (messages d'erreur)

Les messages ICMP

Parmi les messages ICMP qui peuvent être envoyés, citons :

- Host confirmation (Confirmation de l'hôte)
- Unreachable Destination / Service (Destination / service inaccessible)
- Time exceeded (Délai dépassé)
- Route redirection (Redirection de la route)
- Source Quench (Épuisement de la source)

Les messages ICMP

Host Confirmation (Confirmation de l'hôte)

- Un message ICMP Echo (Écho ICMP) permet de déterminer si un hôte est fonctionnel. L'hôte local envoie un message ICMP Echo Request (Demande d'écho) à un autre hôte. L'hôte qui reçoit le message d'écho répond par un message ICMP Echo Reply (Réponse d'écho)

Unreachable Destination or Service (Destination ou service inaccessible)

- Le message ICMP Destination Unreachable (Destination inaccessible) permet de signaler à un hôte que la destination ou le service est inaccessible. Lorsqu'un hôte ou une passerelle reçoit un paquet qu'il ne peut pas livrer, il peut envoyer un paquet ICMP Destination Unreachable à l'hôte source. Le paquet contient des codes qui indiquent pourquoi le paquet n'a pas pu être remis.

  Les codes de destination inaccessible :

  0 = réseau inaccessible
  1 = hôte inaccessible
  2 = protocole inaccessible
  3 = port inaccessible
  4 = Fragmentation nécessaire et flag DF *(Don't Fragment)* activé

Les messages ICMP

Time Exceeded (Délai dépassé)

- Un message ICMP Time Exceeded (Délai dépassé) est envoyé par un routeur pour indiquer qu'il ne peut pas acheminer un paquet car le champ TTL du paquet a expiré. Si le routeur reçoit un paquet et décrémente le champ TTL du paquet jusqu'à zéro, il abandonne le paquet. Le routeur peut également envoyer un message ICMP Time Exceeded à l'hôte source pour l'informer.

Redirection de route

- Un routeur peut envoyer un message de redirection ICMP Redirect pour notifier l'hôte sur un réseau, qu'une meilleure route est disponible jusqu'à une destination particulière

Source Quench (Épuisement de la source)

- Le message ICMP Source Quench (Épuisement de la source) permet de demander à l'hôte source de cesser temporairement d'envoyer des paquets. Si un routeur ne dispose pas de suffisamment d'espace tampon pour recevoir les paquets entrants, il rejette les paquets.

ARP (Address Resolution Protocol) rfc826

Le protocole ARP assure deux fonctions de base :

- ✓ la résolution des adresses IPv4 en adresses MAC
- ✓ la conservation en mémoire cache des mappages.

- Quand un paquet est envoyé à la couche liaison de données pour être encapsulé dans une trame, le nœud désigne une table dans sa mémoire pour y trouver l'adresse MAC qui est mappée à l'adresse IPv4 de destination, Cette table est appelée table ARP, ou cache ARP.
- La table ARP est stockée dans la mémoire vive (RAM) du périphérique.
- Chaque entrée ou ligne de la table ARP comporte deux valeurs : une adresse IP et une adresse MAC. La relation entre les deux valeurs s'appelle une mise en correspondance.

ARP (Address Resolution Protocol) rfc826

La table ARP est mise à jour de manière dynamique (2 méthodes) .

1) surveiller le trafic sur le segment du réseau local, Quand un nœud reçoit des trames en provenance du support, il enregistre les adresses IP source et MAC dans la table ARP sous forme de mappage.

2) diffuser une requête ARP

   - La trame contient un paquet de requête ARP comportant l'adresse IP de l'hôte de destination.
   - la trame est identifié par sa propre adresse IP, la destination répond en envoyant un paquet réponse ARP à l'expéditeur.
   - une nouvelle entrée est créée dans la table ARP.

Rôle d'ARP dans les communications à distance

- Si l'hôte IPv4 de destination se trouve sur le réseau local, la trame utilise l'adresse MAC de ce périphérique comme adresse MAC de destination.

- Si l'hôte IPv4 de destination n'est pas sur le réseau local, la trame utilise l'adresse MAC de l'interface du routeur qui sert de passerelle.

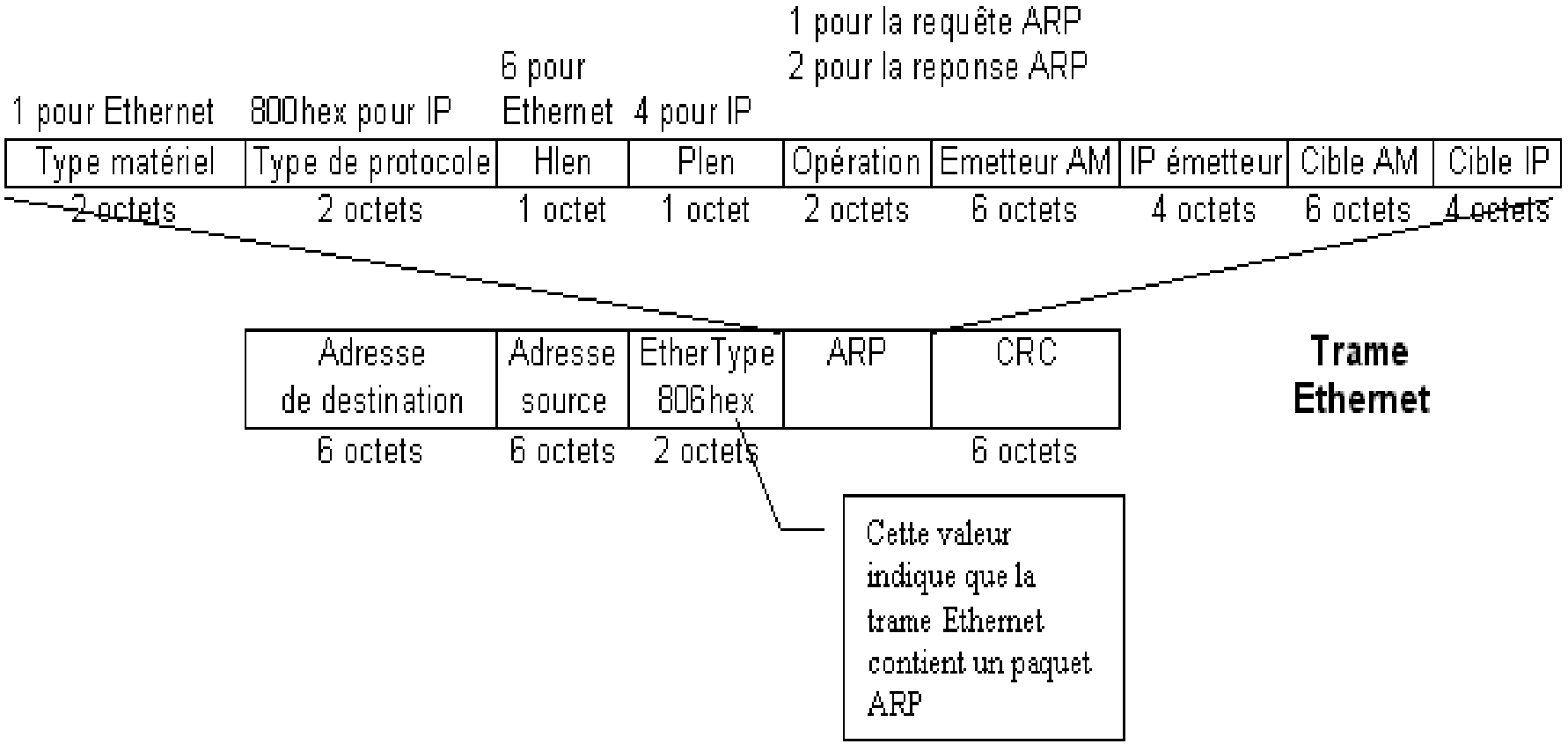
- Si la table ne contient pas d'entrée pour la passerelle, une requête ARP est utilisée pour récupérer l'adresse MAC associée à l'adresse IP de l'interface du routeur.

ARP (Address Resolution Protocol) rfc826

Fonctionnement

Si une machine a besoin de connaître l'adresse Ethernet d'un autre équipement :

1- émission d'une requête ARP (encapsulée dans une trame Ethernet de diffusion, en précisant l'adresse IP du destinataire)



ARP (Address Resolution Protocol) rfc826

Fonctionnement

Les entrées du cache ARP sont horodatées:

- Si le périphérique ne reçoit de trame d'aucun périphérique avant expiration de l'horodatage, l'entrée correspondante est supprimée de la table ARP.
- Certains systèmes d'exploitation Windows stockent les entrées du cache ARP pendant 2 minutes. Si l'entrée est réutilisée pendant ce laps de temps, le compteur ARP de cette entrée passe à 10 minutes.

RARP (Reverse Arp) rfc 2668

- Mécanisme permettant à la station d'obtenir son adresse IP depuis le réseau.
- Permet d'obtenir son adresse IP à partir de l'adresse physique qui lui est associée.
- Comme pour ARP, une trame de diffusion Ethernet est émise, contenant une requête RARP.
- Requête : "*Quelle est l'adresse IP correspondant à mon adresse Ethernet ?*".
- On utilise un serveur RARP sur le réseau physique qui fournit les adresses IP associées aux adresses physiques des stations du réseau. Il envoie une réponse en unicast.

Remarques

- Possible que plusieurs serveurs RARP existent d'où la génération de plusieurs réponses à la requête. La première réponse est considérée.
- Une requête RARP ne peut traverser un routeur. Dans le cas où aucun serveur RARP n'existe sur le réseau physique Ethernet, la requête n'est pas satisfaite.