

Chapitre 6: Protocoles TCP/IP

Sommaire:

Introduction:

Les 4 couches du modèle TCP/IP

Protocoles et équipements du modèle TCP/IP

Description du modèle TCP/IP

Technologie Ethernet:

Protocole TOKEN RING (anneau à jeton)

Technologie FDDI

Fonctionnement des protocoles de transport TCP et UDP

Encapsulation/désencapsulation des données

Structure d'une trame Ethernet:

Adressage IP

Introduction:

En 1969, le ministère de la défense américain (DOD) et DARPA (Defense Advanced Research Projects Agency) développent un projet de recherche pour créer un réseau à commutation de paquet.

Ce réseau appelé ARPANET , a été conçu pour étudier et tester les techniques permettant d'obtenir des transmissions de données, fiables indépendantes du fournisseur.

Le modèle TCP/IP est une architecture réseau en 4 couches, dans laquelle les protocoles TCP et IP jouent un rôle important:

- Un protocole de transport, TCP (Transmission Control Protocol)
- Un protocole réseau, IP (Internet Protocol).

Le modèle TCP/IP, s'est progressivement imposé comme modèle de référence au lieu du modèle OSI.

Il a alors été convenu qu'ARPANET utiliserait la technologie de commutation par paquet (mode datagramme), une technologie émergente promettante.

Introduction:

Les protocoles TCP/IP représentent un ensemble de règles de communication sur internet et se basent sur la notion adressage IP.

C'est-à-dire le fait de fournir une adresse IP à chaque machine du réseau afin de pouvoir acheminer des paquets de données.

Etant donné que la suite de protocoles TCP/IP a été créée à l'origine dans un but militaire, elle est conçue pour répondre à un certain nombre de critères, parmi lesquels :

- Le fractionnement des messages en paquets;
- L'utilisation d'un système d'adresses;
- L'acheminement des données sur le réseau (routage);
- Le contrôle des erreurs de transmission de données.

Le succès de TCP/IP, s'il vient d'abord d'un choix du gouvernement américain, s'appuie ensuite sur des caractéristiques intéressantes :

1. C'est un protocole ouvert, les sources sont disponibles gratuitement et ont été développées indépendamment:

- D'une architecture particulière
- D'un système d'exploitation particulier
- D'une structure commerciale propriétaire.

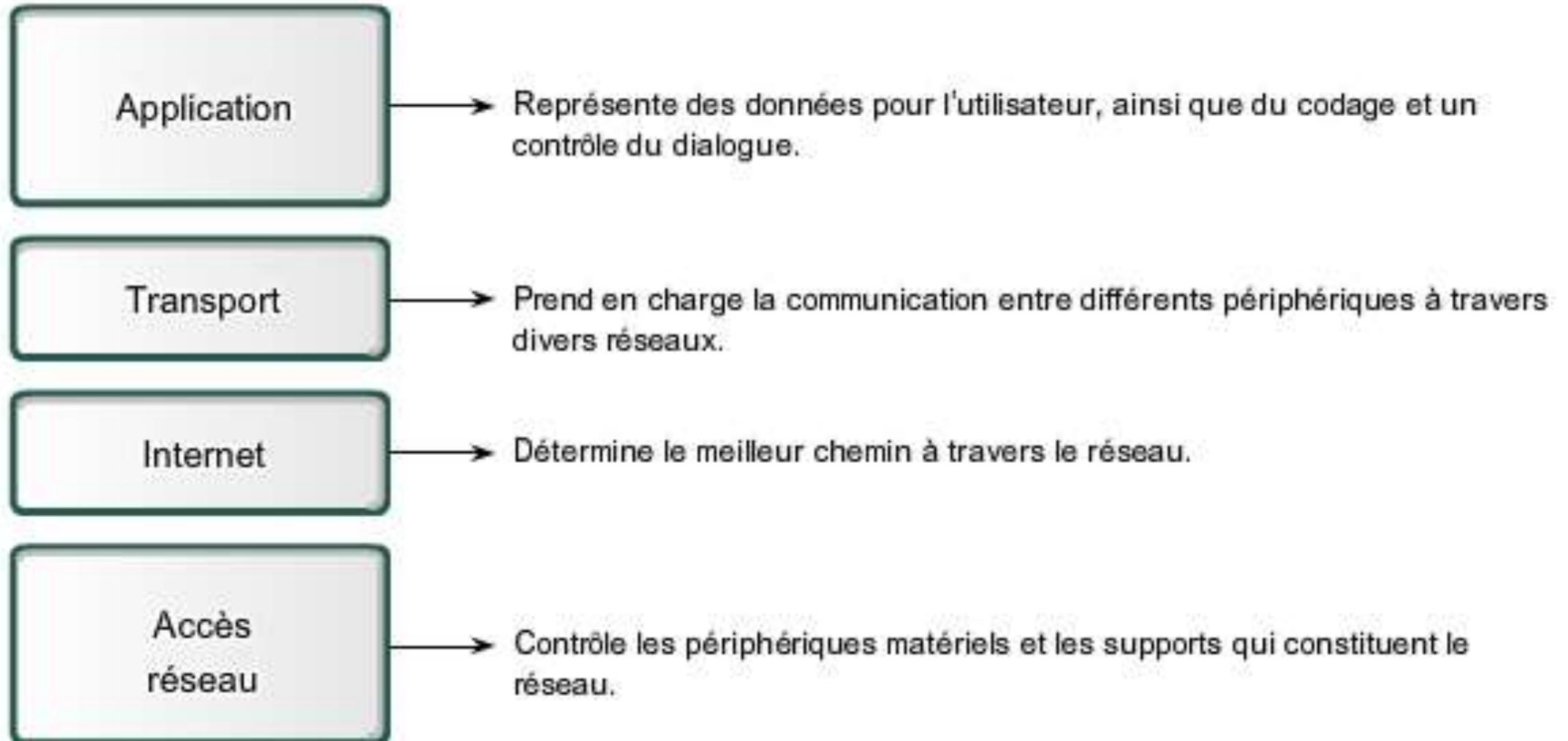
Ils sont donc théoriquement transportables sur n'importe quel type de plate-forme

2. Ce protocole est indépendant du support physique du réseau. Cela permet à TCP/IP d'être véhiculé par des supports et des technologies différents: un câble coaxial Ethernet, un réseau token-ring, une liaison radio (satellites, " Wireless "), une liaison par rayon laser, infrarouge, fibre optique. . .

3. Le mode d'adressage est commun à tous les utilisateurs de TCP/IP quelle que soit la plate-forme qui l'utilise. Si l'unicité de l'adresse est respectée, les communications aboutissent même si les hôtes sont aux antipodes.

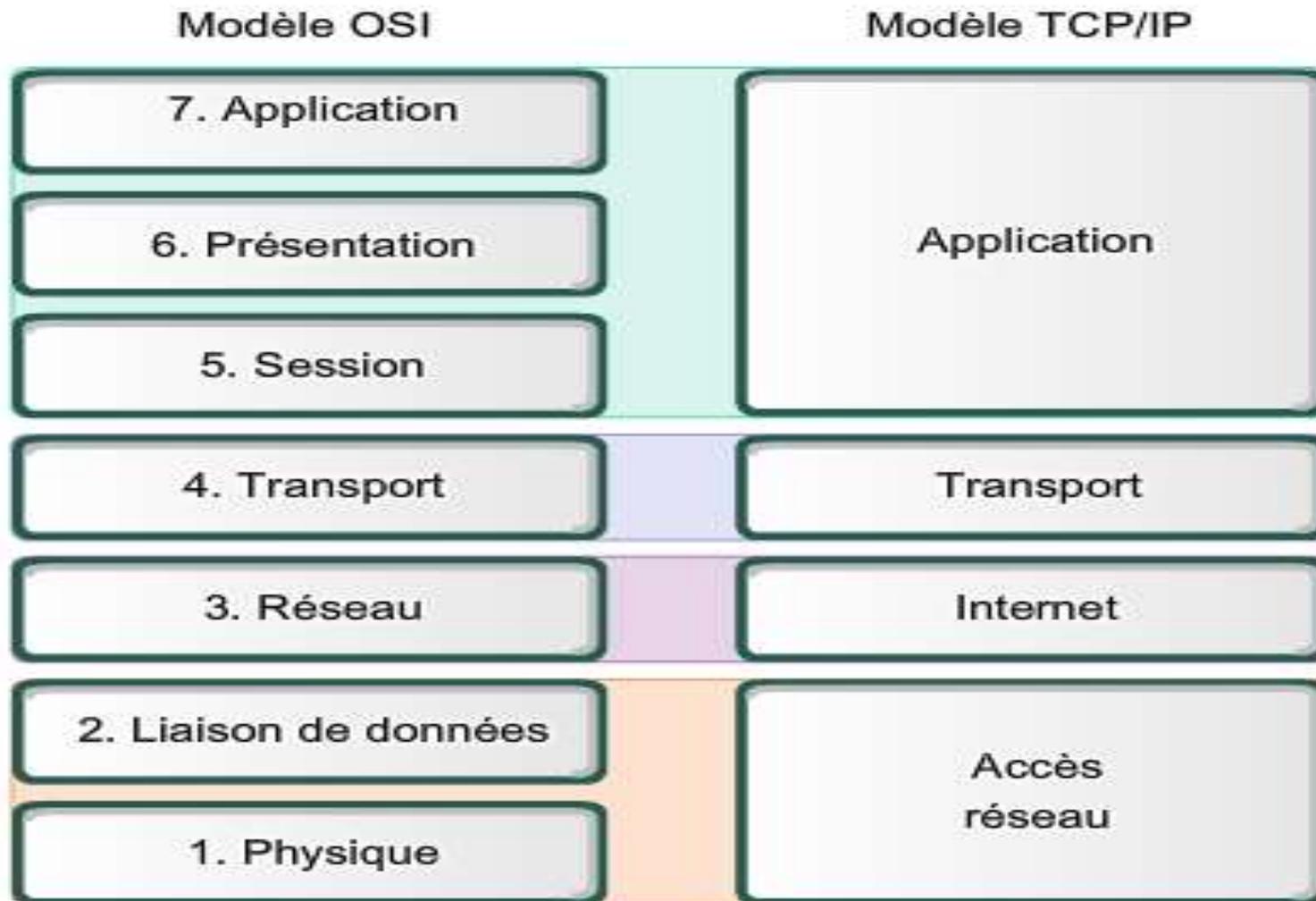
4. Les protocoles de hauts niveaux sont standardisés, ce qui permet des développements largement répandus et inter-opérables sur tous types de machines.

Les 4 couches du modèle TCP/IP



Le modèle TCP/IP ne correspond pas exactement au modèle OSI. TCP/IP combine plusieurs couches OSI en une couche unique et n'utilise pas certaines couches.

Comparaison des modèles OSI et TCP/IP



Les principaux parallèles concernent les couches transport et réseau.⁷

Périphérique / Description

Modèle TCP/IP



Services applicatifs au plus proche des utilisateurs



Encode, encrypte, compresse les données utiles



Etablit des sessions entre des applications



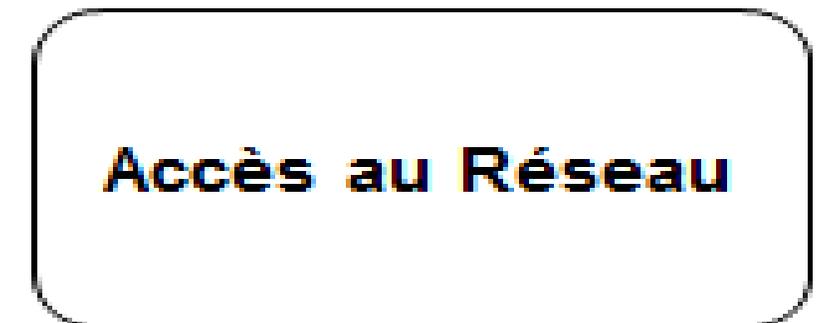
Etablit, maintien et termine les sessions entre périphériques terminaux



Adresse les interfaces globalement et détermine les meilleurs chemins à travers un inter-réseau

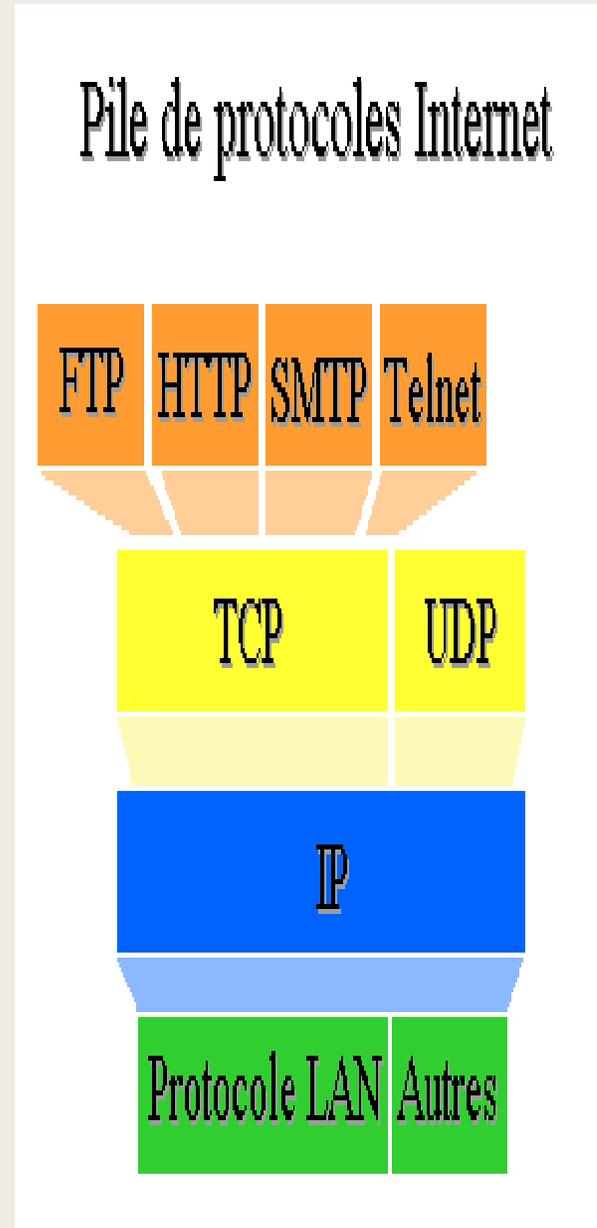


Adresse localement les interfaces, livre les informations localement, via l'utilisation de MAC



Encodage du signal, câblage et connecteurs, spécifications physiques

Les protocoles de chaque couches du modèle TCP/IP



Couches applicatives
(Application, Présentation, Session)

- Messagerie
- Transfert de fichiers
- Internet

Transport

- Contrôle des flots de données
- Accusés de réception

Internet
(Réseau)

- Adressage logique
- Correspondance avec l'adressage physique

Accès réseau
(Liaison de données, Physique)

- Interface physique avec le réseau
- Contrôle d'erreurs

Description de chaque couche du modèle TCP/IP

Le modèle TCP/IP et ses protocoles ont été développée 10 ans avant la définition du modèle OSI.

les fonctionnalités des protocoles de couche application de la norme TCP/IP sont équivalentes à la structure des trois couches supérieures du modèle OSI : les couches application, présentation et session.

La couche Accès réseau:

La couche accès réseau est la première couche de la pile TCP/IP.

- ❑ Elle spécifie la forme sous laquelle les données doivent être acheminées quel que soit le type de réseau utilisé.
- ❑ Elle offre les capacités à accéder à un réseau physique quel qu'il soit, c'est-à-dire les moyens à mettre en œuvre afin de transmettre des données via un réseau.
- ❑ Elle contient toutes les spécifications concernant la transmission de données sur un réseau physique, qu'il s'agisse de réseau local (Anneau à jeton (token ring), Ethernet, FDDI (Fiber Distributed Data Interface), de connexion à une ligne téléphonique ou n'importe quel type de liaison à un réseau.

Elle prend en charge les notions suivantes :

- ✓ Acheminement des données sur la liaison
- ✓ Coordination de la transmission de données (synchronisation)
- ✓ Format des données
- ✓ Conversion des signaux (analogique/numérique)
- ✓ Contrôle des erreurs à l'arrivée...

L'ensemble de ces tâches est en fait réalisé par le système d'exploitation, ainsi que les drivers du matériel permettant la connexion au réseau (ex : driver de carte réseau).

Les protocoles de la couche accès réseau:

Ethernet:

Mise au point par la société XEROX, l'architecture Ethernet est maintenant la solution la plus utilisée pour interconnecter des machines en réseau local.

La technologie Ethernet dispose de ses propres caractéristiques en matière de câblage, de normes, de formats de trame et de méthode d'accès.

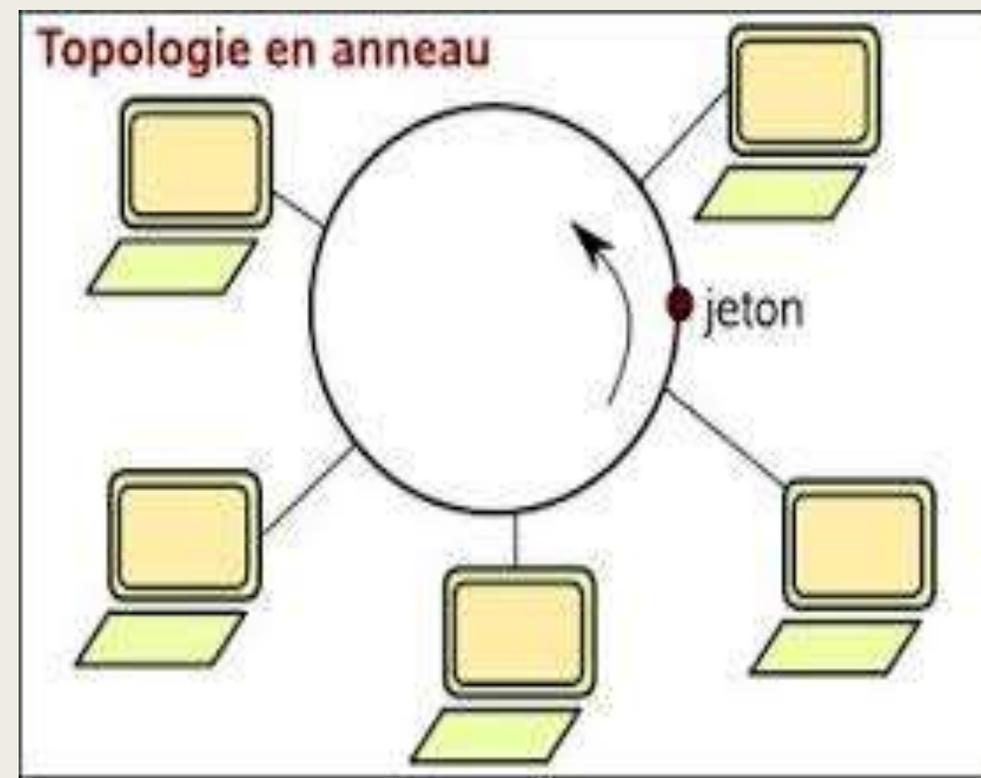
Les caractéristiques principales sont :

- Débit de 10Mbits/s et 100Mbits/s
- Topologie en bus
- Méthode d'accès CSMA/CD
- Longueur des trames comprises entre 64 et 1518 octets.
- Câbles de type coaxial, paire torsadée ou fibre optique (câblage bus ou étoile).
- Protocole de transmission: UDP

Les protocoles de la couche accès réseau:

Protocole TOKEN RING (anneau à jeton)

- A son passage, chaque trame est interceptée par chacune des stations et régénérée.
- Si l'adresse MAC est l'adresse de la station, la trame sera marqué comme lue.
- Après un tour complet (retour à la station émettrice) la trame est supprimée.
- Pour émettre une trame, le station doit posséder le jeton.
- Plusieurs trames peuvent être émises mais le temps de rétention du jeton est fixé.
- Lorsque les envois sont effectués, le jeton est libéré et continue le tour de l'anneau.
- Normalement, la station attend le retour des trames marquées comme lues avant de libérer le jeton (anneau à 4 Mbit/s).
- Pour améliorer la vitesse, le jeton est relâché immédiatement après l'émission (anneau à 16 Mbit/s).



Les protocoles de la couche accès réseau:

Le protocole FDDI (Fiber Distributed Data Interface)

C'est une technologie LAN coûteuse qui utilise une paire (double) d'anneaux de fibre optique.

L'un est l'anneau principal et l'autre est utilisé pour remplacer l'anneau principal en cas de défaillance du réseau.

- FDDI utilise un câble à fibre optique et est câblée dans une topologie en anneau.
- FDDI utilise le jeton comme méthode d'accès au support comme dans le cas du protocole token-ring (anneau) et peut fonctionner à haute vitesse.
- Débit: 100 Mbit/s
- Etendue: 100 KM

La couche internet:

Cette couche est la plus importante dans l'architecture TCP/IP. Elle réalise l'interconnexion des réseaux (hétérogènes) distants sans connexion.

C'est elle qui définit les paquets (datagrammes), et qui gère les notions d'adressage IP.

Son rôle est de permettre l'injection de paquets dans n'importe quel réseau et l'acheminement des ces paquets indépendamment les uns des autres jusqu'à destination.

Comme aucune connexion n'est établie au préalable, les paquets peuvent arriver dans le désordre ; le contrôle de l'ordre de remise est éventuellement la tâche des couches supérieures.

Elle permet l'acheminement des datagrammes (paquets de données) vers des machines distantes ainsi que de la gestion de leur fragmentation et de leur assemblage à réception.

La couche Internet contient 5 protocoles:

Le protocole IP (Internet Protocol): permet la gestion et l'acheminement des paquets d'une machine à une autre, ainsi que l'adressage.

Le protocole ARP (Address Resolution Protocol) : il permet de connaître l'adresse physique d'une carte réseau correspondant à une adresse IP, c'est pour cela qu'il s'appelle Protocole de résolution d'adresse.

Le protocole ICMP (Internet Control Message Protocol): il est principalement utilisé pour déterminer si les données atteignent ou non la destination voulue dans les meilleurs délais. Généralement, le protocole ICMP est utilisé sur des périphériques réseau, tels que des routeurs.

Le protocole RARP(pour Reverse ARP): permet à partir d'une adresse matérielle (adresse MAC) de déterminer l'adresse IP d'une machine.

Le protocole IGMP (Internet group management protocol): c'est le responsable de l'organisation des groupes multicast permettant l'envoi de flux de données IP à plusieurs destinataires.

La couche transport:

Son rôle est le même que celui de la couche transport du modèle OSI : permettre à des entités paires de soutenir une conversation.

Officiellement, cette couche n'a que deux protocoles: le protocole TCP et le protocole UDP (User Datagram Protocol).

TCP est un protocole fiable, orienté connexion, qui permet l'acheminement sans erreur de paquets issus d'une machine d'un internet à une autre.

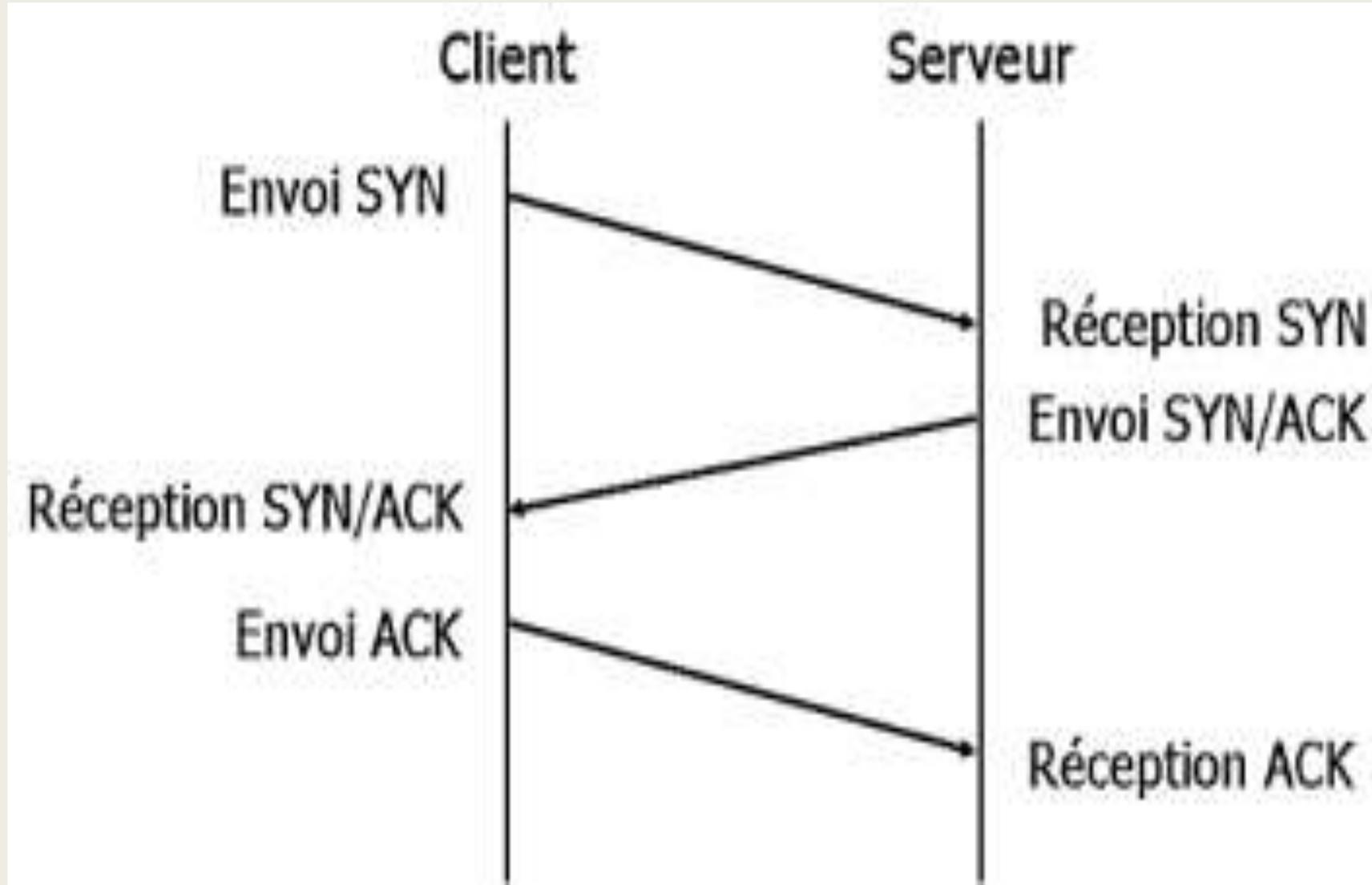
Son rôle est de fragmenter le message à transmettre de manière à pouvoir le faire passer sur la couche internet.

A l'inverse, sur la machine destination, TCP replace dans l'ordre les fragments transmis sur la couche internet pour reconstruire le message initial.

Le protocole UDP est en revanche un protocole plus simple que TCP : il est non fiable et sans connexion.

Fonctionnement des protocoles de transport TCP et UDP:

1. Transmission Control Protocol (TCP)





Le protocole TCP est orienté connexion. Tout d'abord, une session est ouverte entre le client et le serveur.

Après l'ouverture de session, et pour assurer une fiabilisation de transmission, un accusé de réception (ACK - Acknowledgement) répond systématiquement aux paquets.

Le protocole TCP permet de s'assurer de la bonne arrivée de toutes les informations.

En revanche, cette fonction peut ralentir la communication.

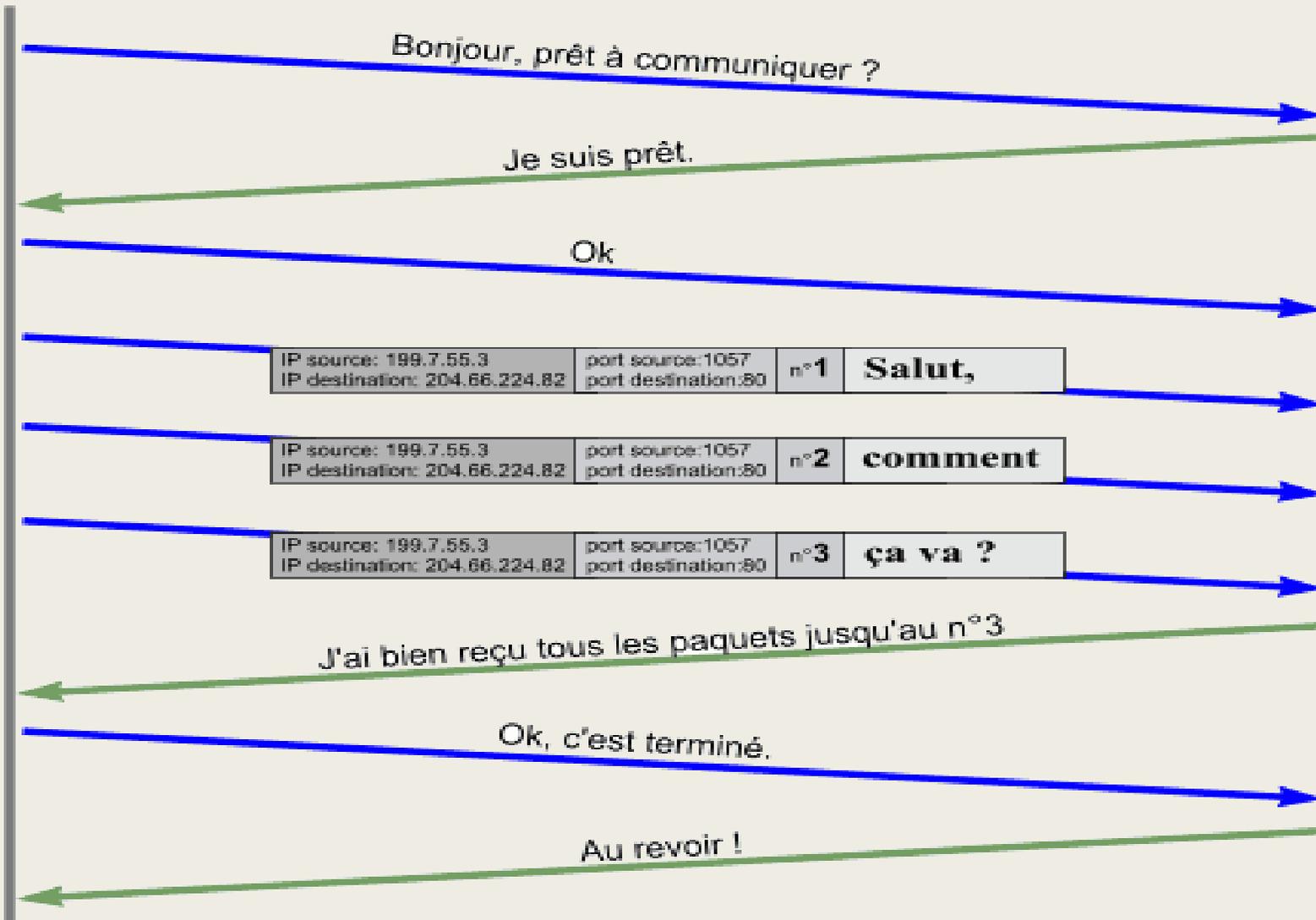
Pour accélérer la transmission et faire en sorte que l'émetteur n'attende pas de recevoir l'accusé de réception pour envoyer l'information suivante, une notion de fenêtre glissante est utilisée.

L'émetteur envoie une rafale d'informations et traite les accusés de réception au fur et à mesure, tout en continuant l'envoi.

Après communication, la connexion est terminée par un dialogue entre le client et son serveur, avec une annonce de fin d'envoi (END) et l'accusé de réception correspondant, pour chaque correspondant.

ordinateur 199.7.55.3

ordinateur 204.66.224.82



User Datagram Protocol (UDP)

UDP est protocole non orienté connexion, non fiable permet d'envoyer des données sans remise d'accusé de réception.

Ainsi les données sont envoyées sans que l'on sache si le destinataire les a bien reçus.

Les messages UDP sont des datagrammes (au lieu de paquets pour TCP) qui sont envoyés individuellement. Les paquets ont des limites définies alors que le flux de données n'en a pas.

UDP prend en charge la détection d'erreur, mais lorsqu'une erreur est détectée, le paquet (datagramme) est rejeté.

La retransmission du paquet pour la récupération de cette erreur n'est pas tentée.

La récupération de l'erreur serait inutile car au moment où le datagramme est retransmis et reçu, il ne sera d'aucune utilité.

UDP est plus rapides que TCP (transmission), de ce fait UDP est généralement destiné aux applications sensibles au temps de réponse telles que les jeux ou la transmission vocale.

L'utilisation du protocole UDP suppose que l'on n'a pas besoin ni du contrôle de flux, ni de la conservation de l'ordre de remise des paquets.

Par exemple, on l'utilise lorsque la couche application se charge de la remise en ordre des messages.

Dans le modèle OSI, plusieurs couches ont à charge la vérification de l'ordre de remise des messages. C'est là un avantage du modèle TCP/IP sur le modèle OSI.

Une autre utilisation d'UDP : la transmission de la voix. En effet, l'inversion de 2 phonèmes ne gêne en rien la compréhension du message final.

De manière plus générale, UDP intervient lorsque le temps de remise des paquets est prédominant.

La couche application:

Contrairement au modèle OSI, c'est la couche immédiatement supérieure à la couche transport, tout simplement parce que les couches présentation et session sont apparues inutiles.

les logiciels réseau n'utilisent que très rarement ces 2 couches, et finalement, le modèle OSI sans de ces 2 couches ressemble fortement au modèle TCP/IP.

Cette couche contient tous les protocoles de haut niveau, comme par exemple Telnet, FTP, TFTP, SMTP, HTTP, DNS...

Le point important pour cette couche est le choix du protocole de transport à utiliser. Par exemple, TFTP (surtout utilisé sur réseaux locaux) utilisera UDP, car on part du principe que les liaisons physiques sont suffisamment fiables et les temps de transmission suffisamment courts pour qu'il n'y ait pas d'inversion de paquets à l'arrivée.

Ce choix rend TFTP plus rapide que le protocole FTP qui utilise TCP. A l'inverse, SMTP utilise TCP, car pour la remise du courrier électronique, on veut que tous les messages parviennent intégralement et sans erreurs.

Les principaux protocoles de la couche application:

DNS (Domain Name Service) : Traduit une adresse internet en adresse IP.

HTTP (Hyper Text Transfer Protocol) : Transfert les fichiers qui constituent les pages web.

HTTPS (Hyper Text Transfer Protocol Secured) : Même rôle que HTTP mais les données sont chiffrées (sécurisés).

FTP (File Transfer Protocol) : Téléchargement fiable de fichiers.

TFTP (Trivial File Transfert Protocole) : Comme FTP, c'est un protocole de téléchargement mais simplifié (moins de fonctionnalités).

SMTP (Simple Mail Transfer Protocol) : Transfert de courriers et de pièces jointes.

TELNET (Teletype Network) : Permet à un client d'effectuer des commandes sur un serveur.

...

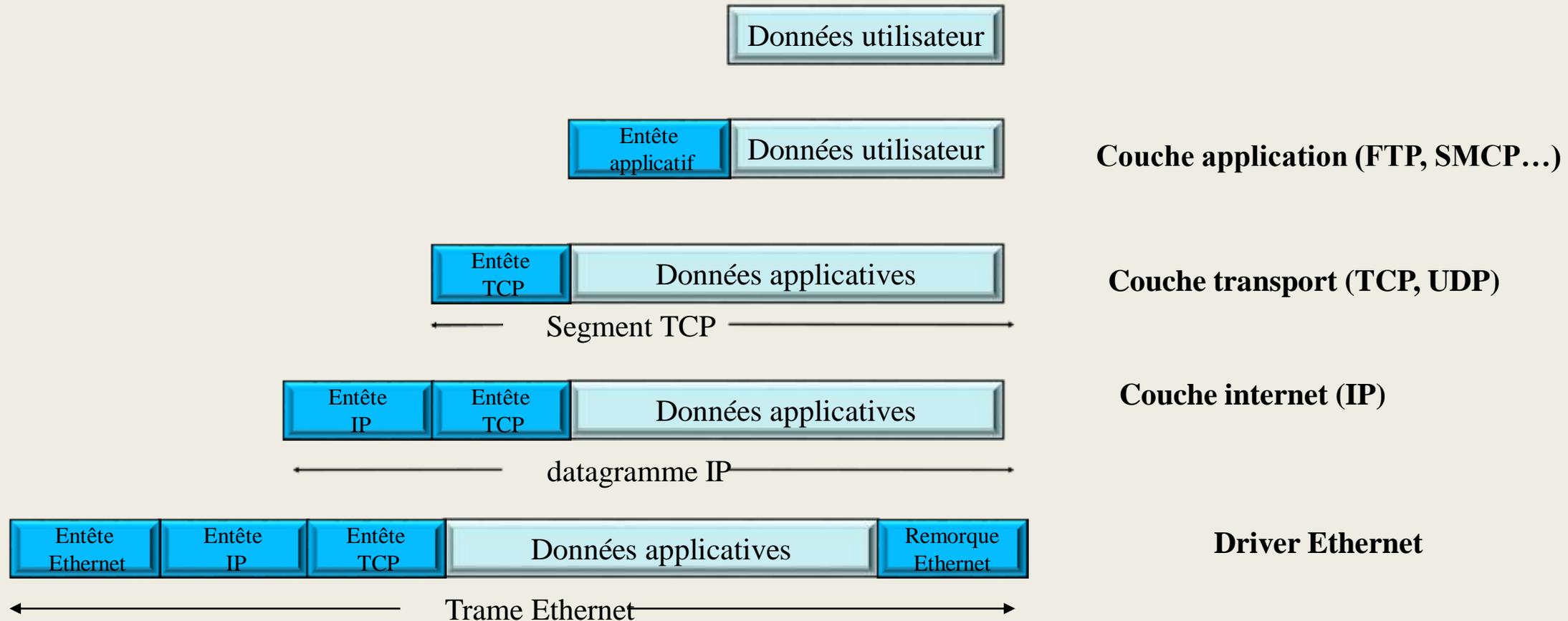
Encapsulation/désencapsulation des données dans le modèle TCP/IP:

Lors d'une transmission, les données traversent chacune des couches au niveau de la machine émettrice.

A chaque couche, une information est ajoutée au paquet de données, il s'agit d'un en-tête, ensemble d'informations qui garantit la transmission.

Au niveau de la machine réceptrice, lors du passage dans chaque couche, l'en-tête est lu, puis supprimé. Ainsi, à la réception, le message est dans son état originel...

Encapsulation / Décapsulation



Encapsulation des données:

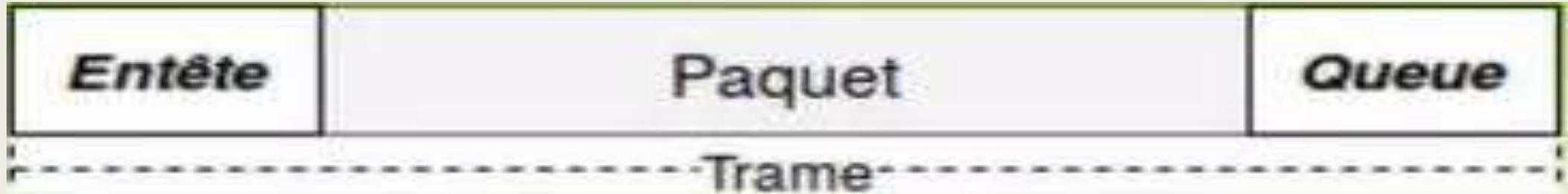
A chaque niveau, le paquet de données change d'aspect, car on lui ajoute un en-tête.

Ainsi les appellations changent suivant les couches :

- Le paquet de données est appelé message (ou donnée) au niveau de la couche Application.
- Le message est ensuite encapsulé sous forme de segment dans la couche Transport.
- Le segment une fois encapsulé dans la couche Internet prend le nom de paquet (ou datagramme).
- Enfin, on parle de trame (frame) au niveau de la couche Accès réseau.

Structure d'une trame Ethernet:

D'une manière générale, une trame se compose de 3 parties principales



1- un en-tête qui contient des informations de contrôle telles que l'adressage.

2- Partie données qui correspond au PDU de la couche 3. pour un réseau TCP/IP c'est un paquet.

3- La queue: fin de la trame qui contient des informations de contrôle pour détecter les erreurs.

Il existe plusieurs types de trames, selon le protocole utilisé.

Structure d'une trame Ethernet:

Preamble	Dest	Source	Length	Type	Data	FCS
8 octets	6 octets	6 octets	2 octets	2 octets	46 à 1500 octets	4 octets

- Preamble: suite binaire qui permet de délimiter le début de la trame et la fin de la trame précédente.
- Adresses destination et source sont au format 48-bit (adresses MAC)
- Length: longueur des données.
- Type: indique le type de protocole utilisé par la couche réseau (IPv4, IPv6, ARP, RARP...).
- Chaque protocole a sa propre structure de paquets.
- FCS (frame check sequence): est le code de détection d'erreurs ajoutées à la fin d'une trame.

Trame Ethernet:

Si le nombre de données n'atteint pas 46 octets, le champ est complété par une séquence de bourrage.

Si les données sont insuffisantes pour former une trame dont la taille est supérieure ou égale à Lmin (46 octets), alors de données de bourrage sont rajoutées à l'émission et elles sont retirées à la réception avant de passer les données utiles à la couche supérieure.

Préambule 7 octets	Délimiteur de début de trame (1 octet)	Adresse MAC Destination (généralement 6 octets)	Adresse MAC Source (généralement 6 octets)	Longueur du champ de données (2 octets)	Données	Bourrage (Complément pour obtenir 46 octets)	Code de contrôle de la trame (4 octets)

Les données de bourrage sont des octets à « 0 »

Adressage IP (Internet Protocol):

Définition d'une adresse IPv4

Une adresse IP identifie de manière unique une machine ainsi que le réseau sur lequel elle est située.

Chaque adresse est une série de quatre octets (8 bits) dont une partie correspond à l'identificateur du réseau et l'autre partie à l'identificateur de la machine

L'adresse IP d'une machine est une adresse réseau codée sur 32 bits.

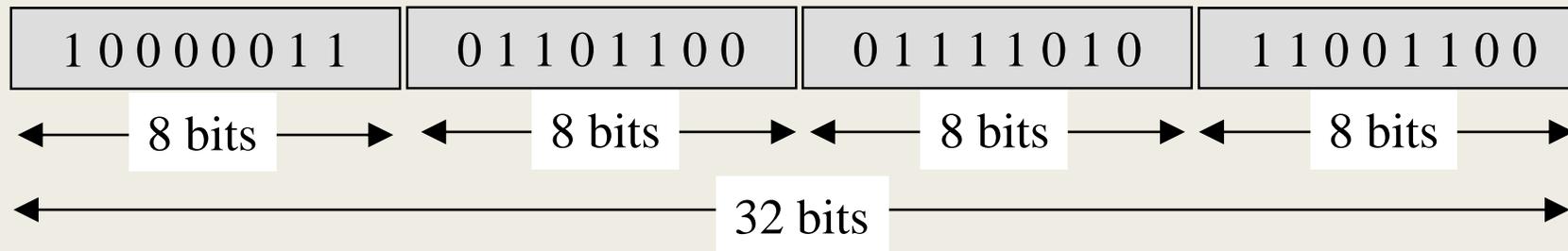
Exemple : 192.93.116.3

Principe de l'adressage:

- Chaque hôte (machine) dispose d'une adresse unique.
- C'est une adresse logique et non physique (différente de l'adresse physique et peut être modifiée).
- L'adresse est assignée à l'interface et non à la machine.
- Les adresses sont groupées par rapport au numéro du réseau (adresse réseau).
- Les interfaces d'un même groupe doivent être connectés au même média (bus, switch, hub).

Adresse IP:

- Chaque combinaison (2^{32} combinaisons) représente une adresse .

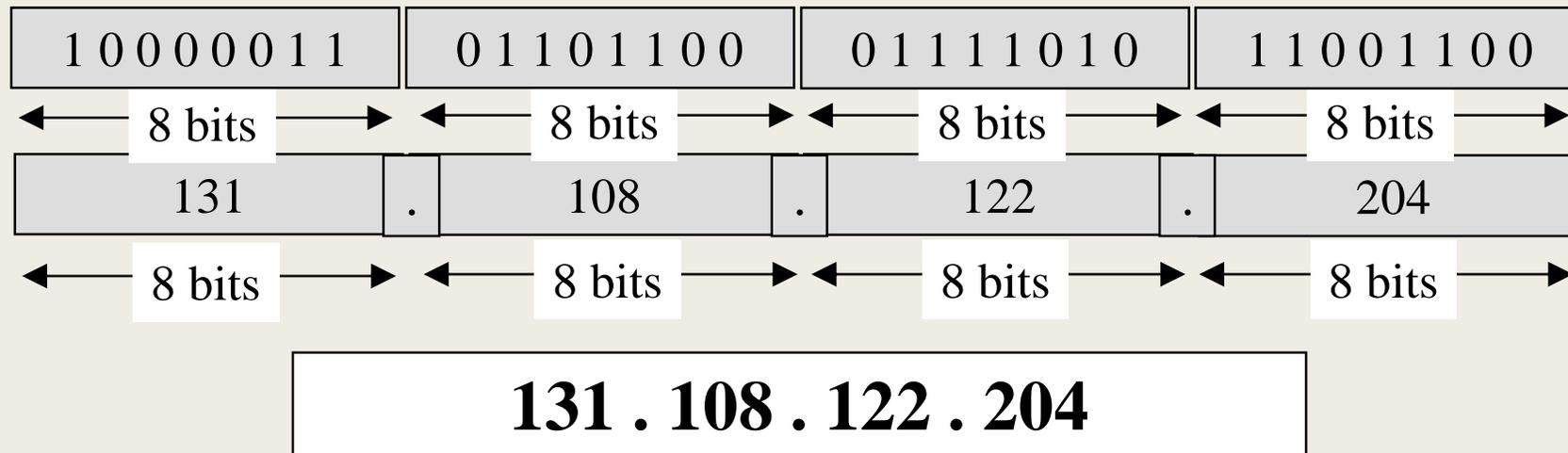


- Une adresse IP est représentée dans un format décimal avec 4 nombres séparés par des points.
- On parle de "notation décimale pointée".

Notation décimale pointée des adresses IP:

- Chaque 8 bits de l'adresse représente un nombre décimal
- Ce nombre décimal représente une valeur entre 0 à 255.

Exemple 1 :



Exemple 2 :

• L'adresse `10000011.01101100.01111010.11001101`
Est représentée par : `131 . 108 . 122 . 205`

• L'adresse : `131 . 108 . 122 . 264` est non valide puisque le dernier nombre est supérieur à 255

Champs d'une adresse IP

Une adresse IP comprend deux parties :

- Un **numéro de réseau** (NET-ID): une adresse globale pour identifier un réseaux, cette adresse est commun a toutes les machines de ce réseau.
- Un **numéro de machine** (hôte) : identifier une machine dans un réseau.



Une adresse = N° réseau + N° machine

Exemple : soit l'adresse **131 . 108 . 122 . 204** , si on considère

k = 16 et n=16 alors :

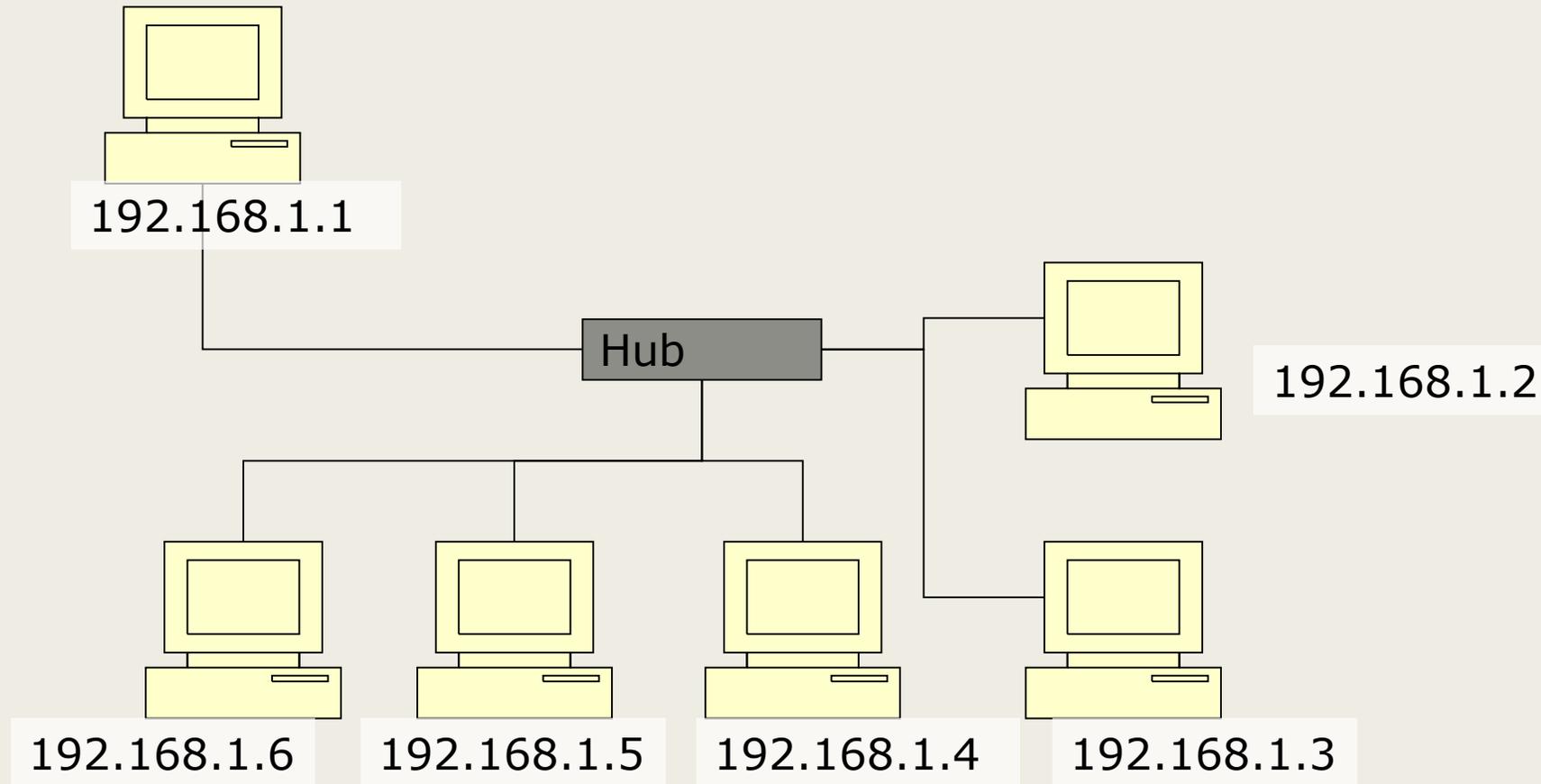
NET-ID : 131.108.0.0

HOST : 0.0.122.204

Exemple : soit le réseau ayant le numéro 192.168.1.0

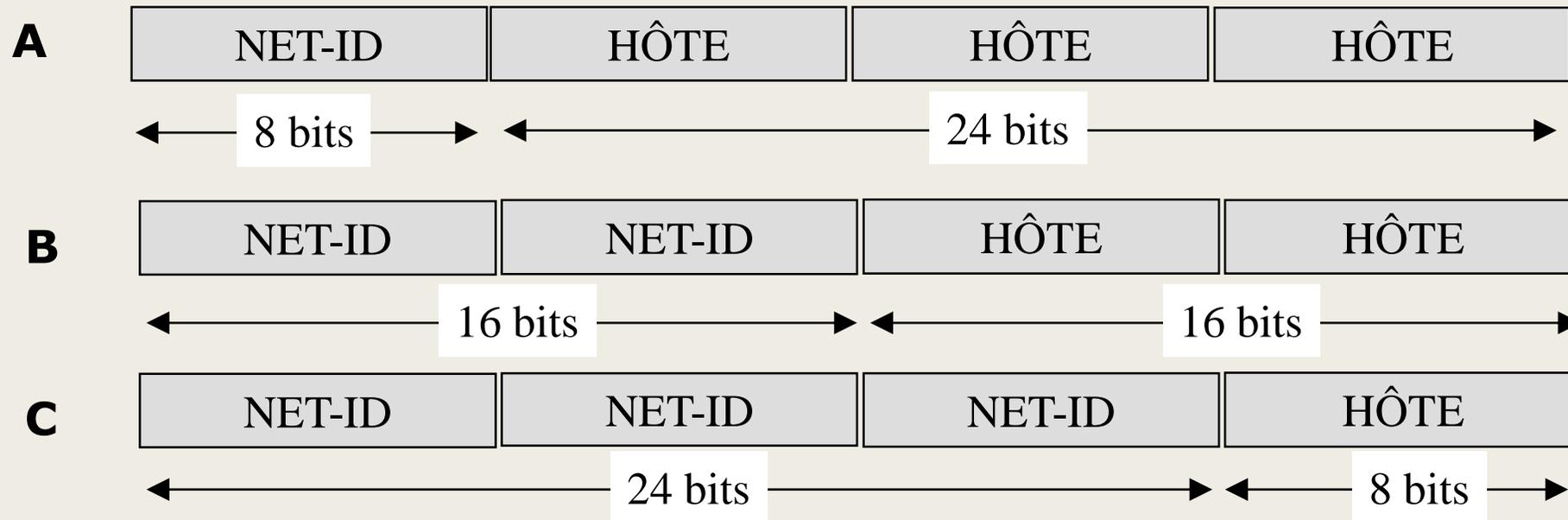
les machines de ce réseaux possèdent les adresses :

192.168.1.1 , **192.168.1.2** , **192.168.1.3** , **192.168.1.4** , **192.168.1.5** , **192.168.1.6**



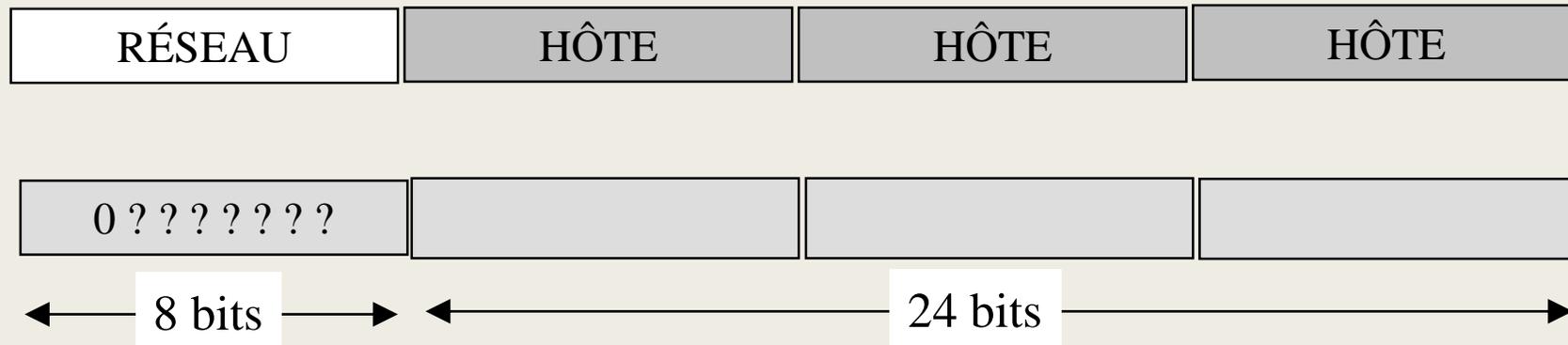
Classes d'adresse IP:

- La taille de la partie réseau (net-id) détermine la classe de l'adresse
- Les adresses IP sont classées en 3 classes :



Adresse IP de classe A:

- Le premier octet est réservé au réseau, les 3 octets (24 bits) suivants sont réservés aux hôtes.
- Les premiers bits des octets réseau sont toujours à 0 (il reste 7 bits).



Nombre de réseaux disponibles : $2^7 = 128$ réseaux

Nombre d'hôtes disponibles : $2^{24} = 16\,777\,216$ hôtes

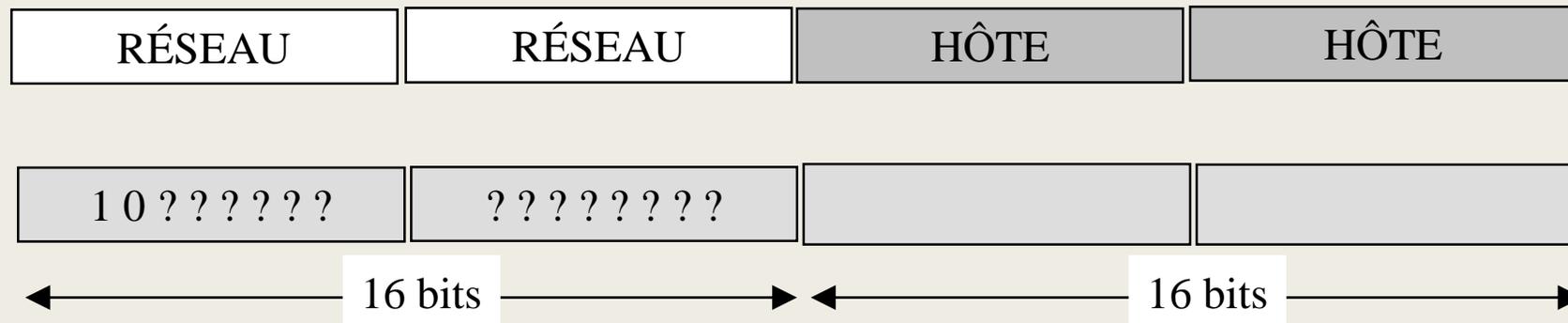
Exemple :

90.25.48.10 correspond à une adresse de classe A

01011010 00011001 00110000 00001010

Adresse IP de classe B:

- Les 2 premiers octets sont réservés au réseau, les 2 octets (16 bits) suivants sont réservés aux l'hôtes.
- Les deux premiers bits des octets réseau sont toujours à 10 (il reste 14 bits)



Nombre de réseaux disponibles : $2^{14} = 16\ 384$ réseaux

Nombre d'hôtes disponibles : $2^{16} = 65\ 536$ hôtes

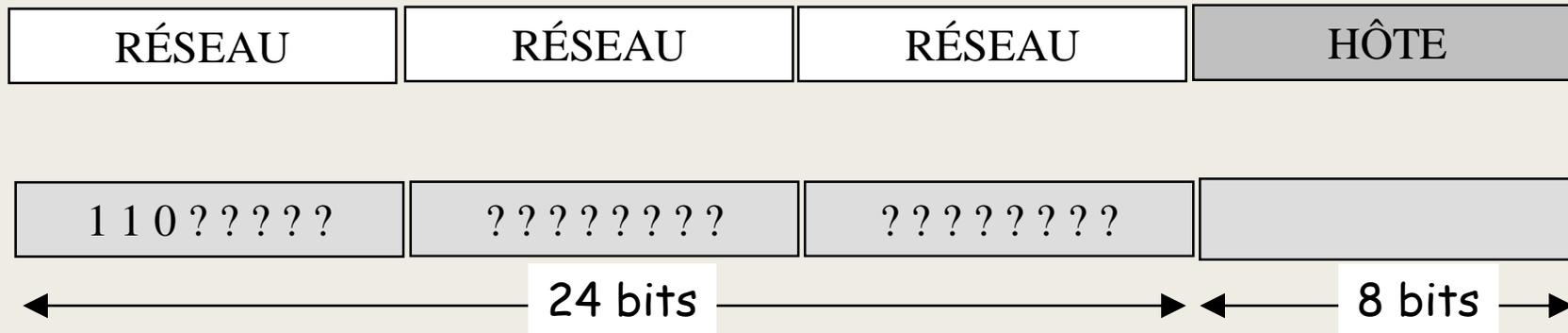
Exemple :

130.100.20.10 correspond à une adresse de la classe B

10000010 01100100 00010100 00001010

Adresse IP de classe C:

- Les 3 premiers octets sont réservés au réseau, l'octet (8 bits) suivant est réservé aux l'hôtes.
- Les trois premiers bits des octets réseau sont 110 (il reste 21 bits)



Nombre de réseaux disponibles : $2^{21} = 209\,752$ réseaux

Nombre d'hôtes disponibles : $2^8 = 256$ hôtes

Exemple :

192.5.5.11 correspond à une adresse de classe C .

11000000 00000101 00000101 00001011