Introduction aux réseaux IP

Sylvain MONTAGNY

sylvain.montagny@univ-savoie.fr

Bâtiment chablais, bureau 13

04 79 75 86 86

Retrouver tous les documents de Cours/TD/TP sur le site
www.master-electronique.com

Présentation cours : Sommaire

- Cours :
  - Chapitre 1 : Topologie et classification des réseaux
  - Chapitre 2 : Le modèle OSI de l'ISO
  - Chapitre 3 : Les équipements d'interconnexion
  - Chapitre 4 : Le protocole Ethernet
  - Chapitre 4 : Couche 3, Les protocoles IP, ARP et ICMP
  - Chapitre 5 : Le routage IP
  - Chapitre 6 : Couche 4, Les protocoles TCP et UDP
  - Chapitre 7 : Les protocoles d'applications

Présentation TD

- TD :
  - TD 1 : Topologie des réseaux et modèle OSI
  - TD2 : Le protocole Ethernet
  - TD3 : Le protocole ARP, Adressage IP
  - TD4 : Le routage IP
  - TD5 : Les protocole UDP et TCP, La translation d'adresse

Présentation TP

- TP :
  - TP1 : Analyse de trames avec LANWATCH, analyse et modification de la configuration IP
  - TP2 : Utilisation d'un simulateur réseau « Packet Tracer »
  - TP3 : Routage statique
  - TP4 : Routage dynamique

Un réseau, c’est quoi ?

- Un réseau informatique est un ensemble d'équipements interconnectés qui servent à partager un flux d’informations.
- **Le partage des ressources :**
  - **Matérielles** : Imprimantes, disque dur, lecteur de CD-ROM, modem, etc…
  - **Logicielles** : Base de données, banque d'images, fichier texte, programme utilisateur, etc…

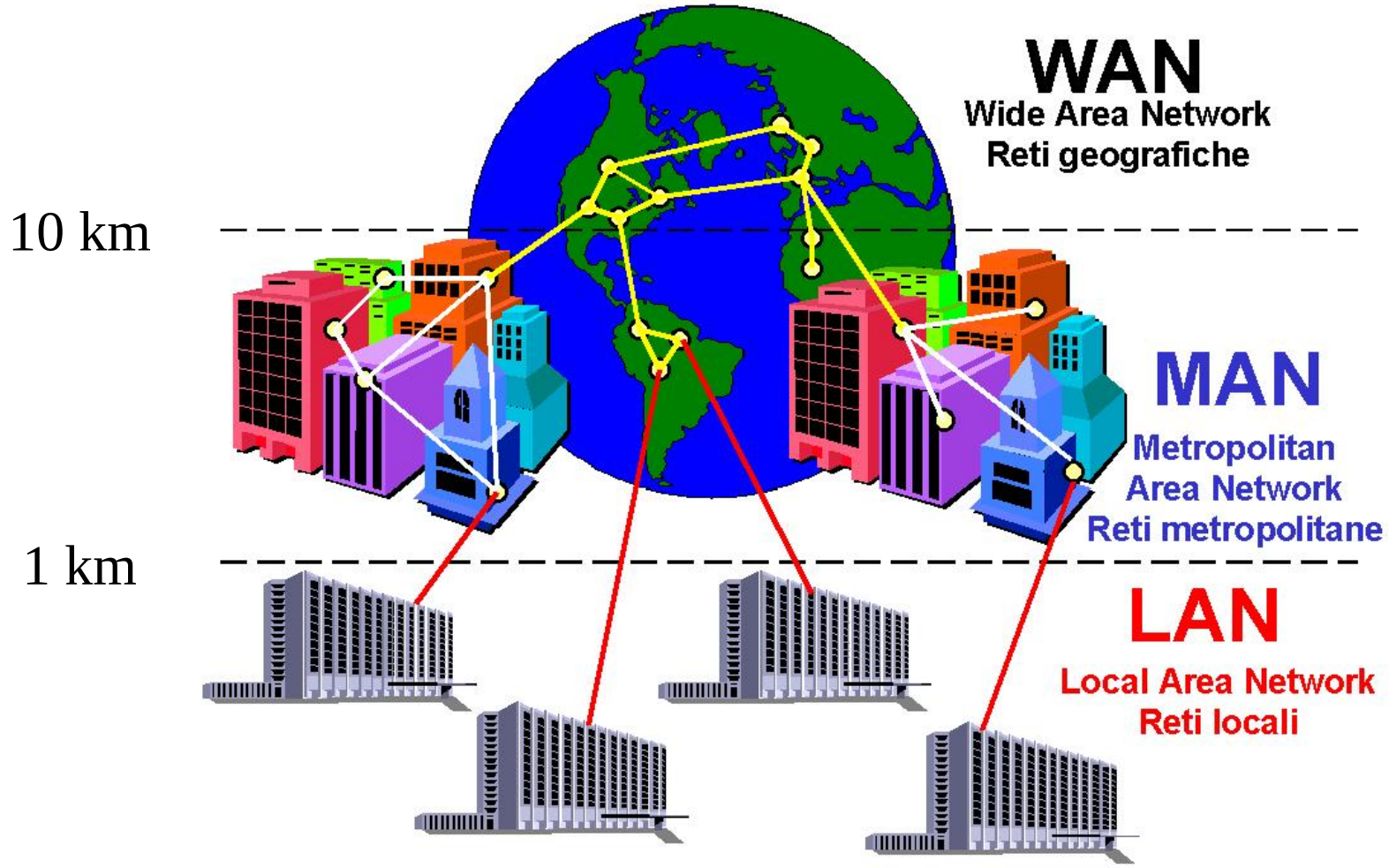
Que faut-il pour construire un réseau ?

- **Des équipements informatiques** : Ordinateurs, imprimantes, serveurs…
- **Des supports de transmissions** : Leur rôle est d'acheminer l'information d'un matériel à un autre en les reliant.
- **Des dispositifs d'interconnexion de réseau** : Pour réunir plusieurs réseaux ou de subdiviser le réseau en plusieurs réseaux.
- **Des systèmes d'exploitation réseau** : Dans certains cas on parlera de logiciel CLIENT et de logiciel SERVEUR.
- **Des protocoles** : l'hétérogénéité des matériels utilisés impose d'utiliser un certain nombre de règles.

Chapitre 1 : Topologie et classification des réseaux

- 1.1 Classification des réseaux : LAN, WAN…
- 1.2 Les supports de transmission
- 1.3 Topologie des réseaux
- 1.4 Caractéristique d'une transmission
- 1.5 Caractéristique des signaux

Classification par la taille



Classification par taille

- **Réseau local** (**LAN** = Local Area Network):

Pour les réseaux limités à une entreprise, une administration. Privé.

- **Réseau métropolitain** (**MAN** = Metropolitan Area Networks):

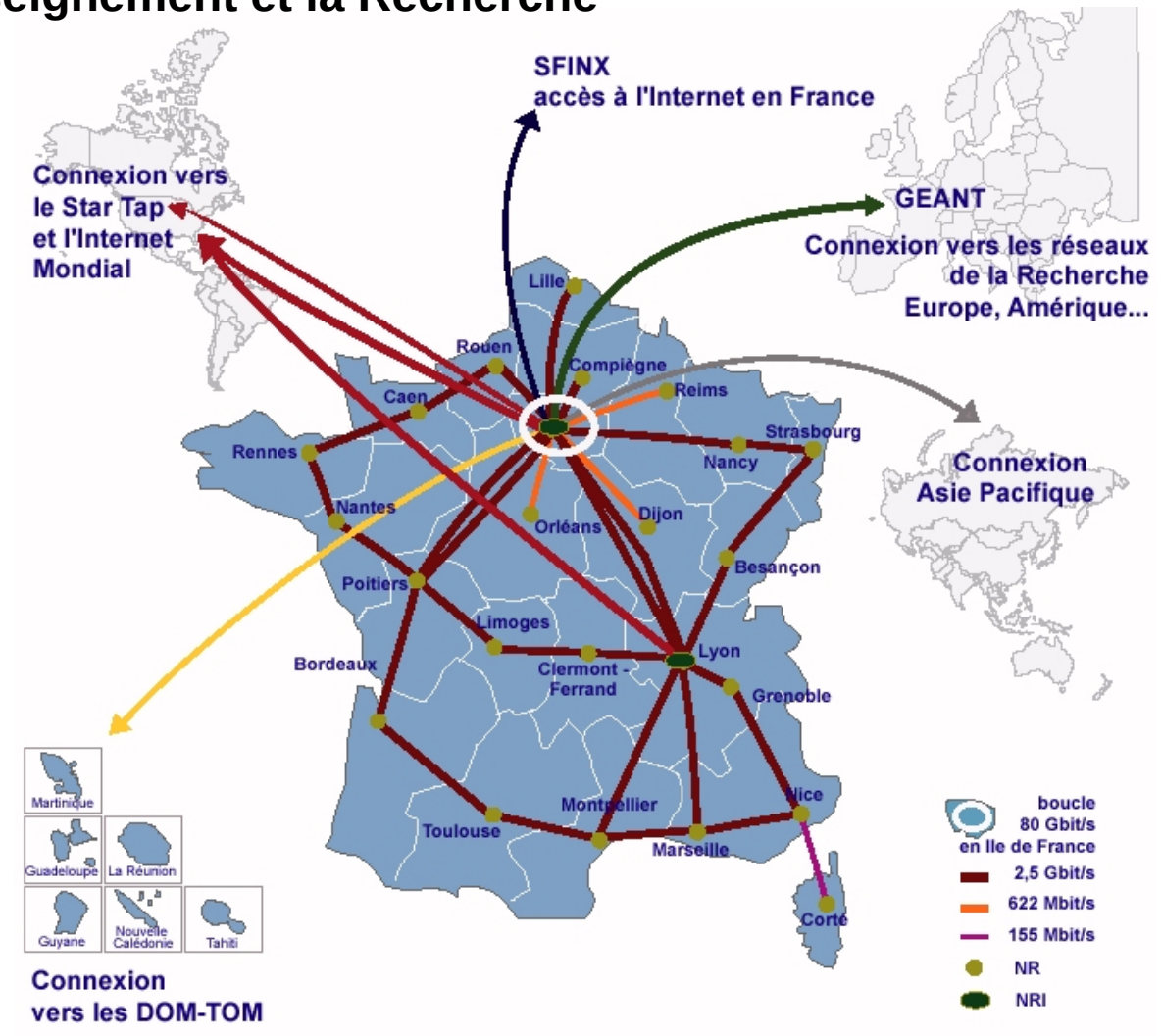
Pour les réseaux pouvant couvrir un grand campus ou une ville.

- **Réseau étendu** (**WAN** = Wide Area Network):

Pour des réseaux reliant des matériels informatiques éloignés les uns des autres (distance mesurée en kms). Echelle de la terre entière.

Exemple de WAN : Renater

Le Réseau National de télécommunications pour la Technologie l'Enseignement et la Recherche



Chapitre 1 : Topologie et classification des réseaux

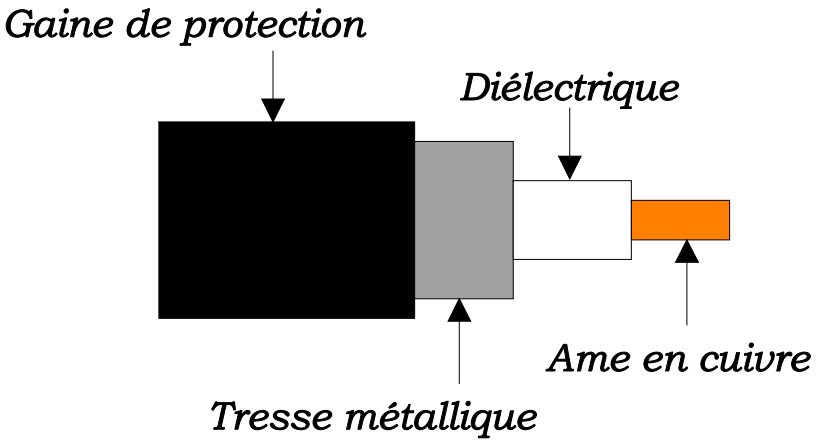
- 1.1 Classification des réseaux : LAN, WAN…
- 1.2 Les supports de transmission
- 1.3 Topologie des réseaux
- 1.4 Caractéristique d'une transmission
- 1.5 Caractéristique des signaux

Caractéristiques

- **Débit maximal :** Nombre de bits/seconde pouvant être transporté sur le support. Dépend des caractéristiques physiques du matériau.
- **Type du signal véhiculé :** Electrique, lumineux ou ondes électromagnétiques.
- **Atténuation :** En dB/m. Affaiblissement du signal le long de la ligne.
- **La sensibilité aux perturbations électromagnétiques**
- **Les coûts** : Fabrication et installation

Les câbles coaxiaux (1)

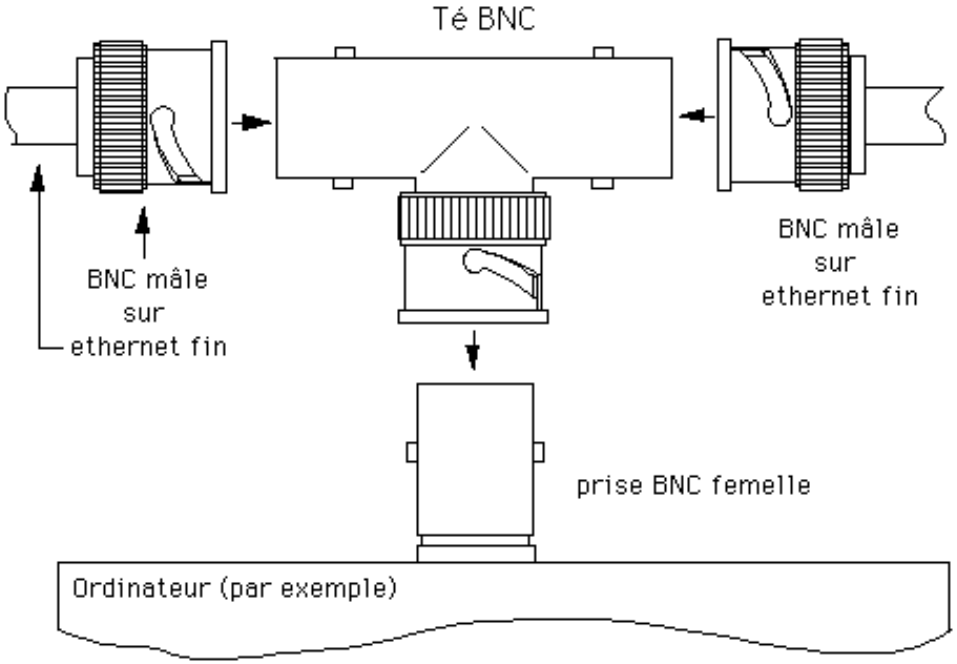
- **Premier** type de **câble** utilisé dans les réseaux locaux type **Ethernet.**
- Composé de **deux conducteurs** cylindriques de même axe, séparés par un **isolant.**



- Permet d'**isoler** la transmission des **perturbations** dues aux **"bruits" extérieurs.**

Les câbles coaxiaux (2)

- le câble coaxial **fin** (thin) lié à la norme Ethernet **10Base2**, câble plus souple et moins cher. Les connexions sont réalisées avec des **prises BNC**.



Câble coaxial

T de raccordement

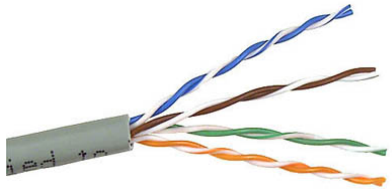
Bouchon 50 Ω

Caractéristiques des câbles coaxiaux

- **Débit :** Entre 10 Mbps et 100 Mbps (sur de courtes distances).
- **Pose relativement facile** moyennant quelques précautions (pas d'angles trop aiguës : rayon de courbure minimum de 5 cm pour le fin et de 30 cm pour l'épais), par contre les **modifications** (ajout ou retrait de noeuds) sont beaucoup **moins faciles** à effectuer qu'avec de la paire torsadée.
- **Coût faible:** Environ 2 €/m.

Les câbles à paires torsadées (1)

- **Provient** du monde de la **téléphonie**. Les **fils** de cuivre ou d'aluminium des différentes paires sont **isolés** les uns des autres par du plastique et enfermés dans une gaine.



- Support de transmission constitué de **paires de fils** électriques (généralement 4 paires), l'une servant à l'**émission**, une autre à la **réception**, les deux dernières étant réservées aux commandes.
- Chaque paire est **torsadée** sur elle même, afin d'éviter les phénomènes de **diaphonie** (interférence entre conducteurs).
- Il existe des câbles **blindés** (STP) ou non **blindés** (UTP).
- Défini dans la norme **10BaseT**, ce type de câbles est utilisé pour du câblage dit universel mais aussi pour les réseaux à topologie en anneau ou étoile.

Les câbles à paires torsadées (2)

Câble à paires torsadées

Prise RJ45

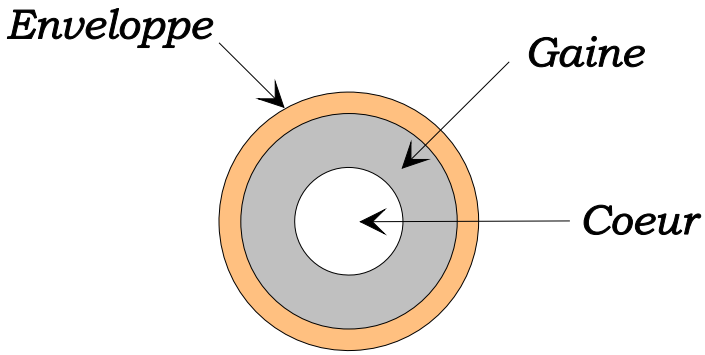
Connecteur RJ45 sur carte réseau

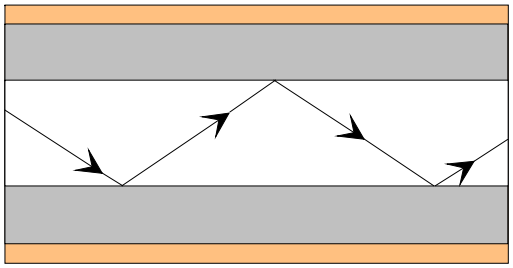
Caractéristique des câbles à paires torsadées

- **Atténuation : De l'ordre de 20dB/km**
- **Débit relativement important:** de 10 jusqu'à 100 Mbps sur de courtes distances.
- **Perturbation** électromagnétique possible (un blindage permettra de palier à ce problème).
- **Pose très facile**.
- Coût : le **moins cher** du marché (< 2 €/m).

La fibre optique

- Technologie relativement **récente** (les premiers essais datent de 1972).
- Le principe: **propagation de la lumière** dans un milieu protégé assurant un **minimum d'atténuation**.
- Une fibre optique est composée de 2 substances (silice plus ou moins dopée) d'**indices** de réfraction **différents** (principe du miroir) : le cœur et la gaine. Les rayons lumineux sont donc emprisonnés dans le cœur.





La fibre optique

- Support de transmission utilisé pour des liaisons **longues distances et insensible aux perturbations électromagnétiques**, défini dans la norme 10BaseF.

Caractéristiques des fibres optiques

- **Atténuation :** de l'ordre de 0.15 dB/km
- **Vitesses** de transmission **très élevées**, débit maximum le meilleur : 1 Giga bits par seconde.
- **Pose délicate** (matériau rigide, angles de courbures importants)
- **Coût élevé** : 10 €/mètre environ, technologie coûteuse des convertisseurs optique-numérique.
- **Pas d'échauffement** (à haute fréquence le cuivre chauffe, il faut le refroidir pour obtenir des débits très élevés).
- **Poids au mètre faible** (facteur important, aussi bien pour réduire le poids qu'exercent les installations complexes dans les bâtiments, que pour réduire la traction des longs câbles à leurs extrémités).

Conclusion: Norme et type de conducteur

	100 m	1 km	5 km	50 km
10 Gb/s	10 GBase-SX *multimode*	10 Gbase-Lx *multimode*	10 GBase-LX *monomode*	10 GBase-EX *monomode*
1 Gb/s	1 GBase-T *cuivre*	1 GBase-SX *multimode*	1 GBase-LX *monomode*	
100 Mb/s	100 Base-Tx *cuivre*	100 Base-FX *multimode*		
10 Mb/s	10 Base-T *cuivre*	10 Base-F *multimode*		

Norme Ethernet et type de conducteur suivant les distances et les débits requis
doc. Yalta

Ondes électromagnétiques

- Les réseaux sans fil permettent de relier très **facilement** des équipements distants d'une dizaine de mètres à quelques kilomètres. **L'installation** de tels réseaux ne demande pas de lourds aménagements des infrastructures existantes.

- **Utilisées** pour un grand nombre d'applications (militaires, scientifiques, amateurs, ...), **sensibles** aux interférences, les transmissions d'ondes électromagnétiques sont soumises à une **forte réglementation**.

- Ces ondes étant difficiles à confiner dans une surface géographique restreinte, il est facile d'espionner un réseau basé sur ce type de transmissions.

Les réseaux « sans-fil »

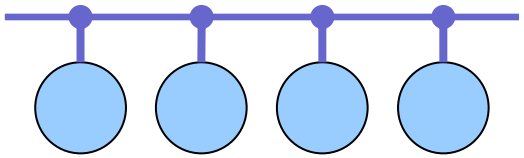
- **WPAN** (*Wireless Personal Area Network*) : réseaux sans fil de faible portée, technologie dominante **« Bluetooth »**.
- **WLAN** (*Wireless Local Area Network*) permet de couvrir l'équivalent d'un réseau local d'entreprise. Technologies concurrentes: Le **WIFI** (ou IEEE 802.11)
- **WMAN** (*Wireless Metropolitan Area Network*) connu sous le nom de **Boucle Locale Radio** (*BLR*), principalement destiné aux opérateurs de télécommunication.
- **WWAN** (*Wireless Wide Area Network*) connu sous le nom de **réseau cellulaire mobile**. Les principales technologies sont:
  - **GSM** (*Global System for Mobile Communication* ou en français *Groupe Spécial Mobile*).
  - **GPRS** (*General Packet Radio Service*).
  - **UMTS** (*Universal Mobile Telecommunication System*).

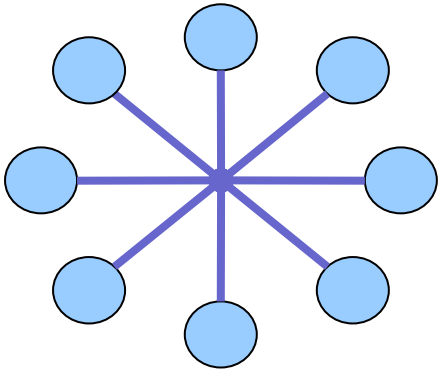
Chapitre 1 : Topologie et classification des réseaux

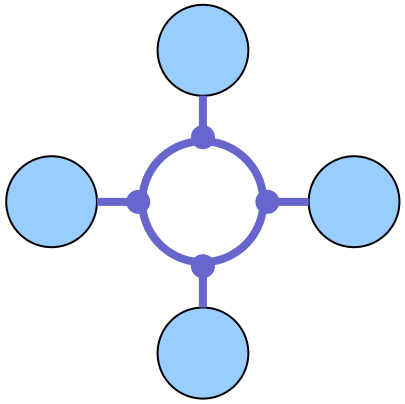
- 1.1 Classification des réseaux : LAN, WAN…
- 1.2 Les supports de transmission
- 1.3 Topologie des réseaux
- 1.4 Caractéristique d'une transmission
- 1.5 Caractéristique des signaux

La topologie des réseaux

- Il s'agit de la façon dont les ordinateurs sont interconnectés entres eux :
  - En Bus
  - En Etoile
  - En anneau

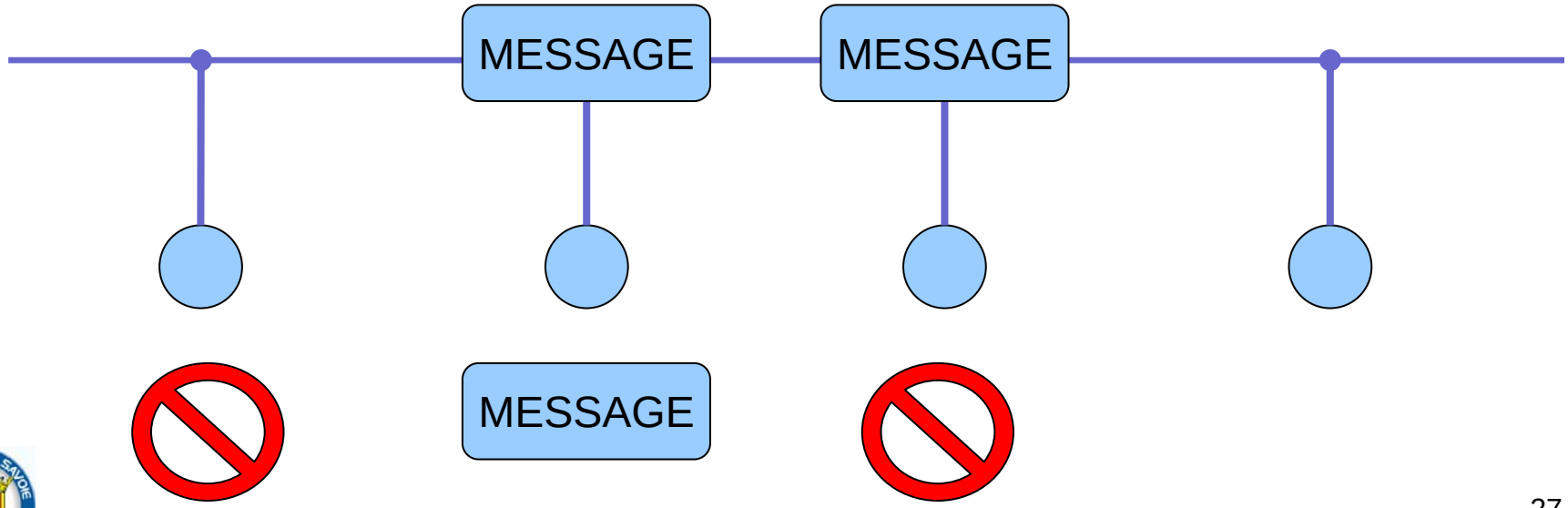






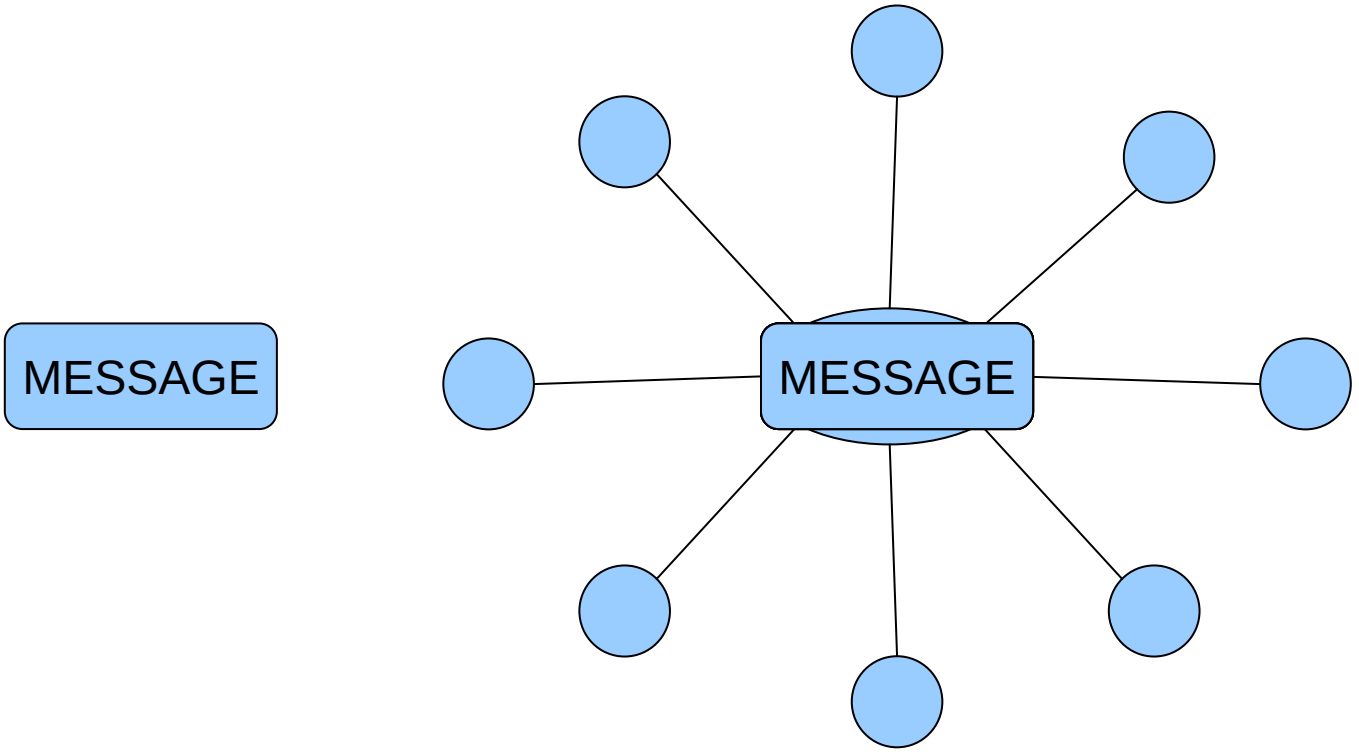
En Bus

- Une **topologie en bus** est l'organisation la plus simple d'un réseau. En effet, dans une topologie en bus tous les ordinateurs sont reliés à une même ligne de transmission par l'intermédiaire de câble, généralement coaxial. Le mot « bus » désigne la ligne physique qui relie les machines du réseau.
- Cette topologie a pour avantage d'être facile à mettre en œuvre et de posséder un fonctionnement simple. En revanche, elle est extrêmement vulnérable étant donné que si l'une des connexions est défectueuse, l'ensemble du réseau en est affecté.



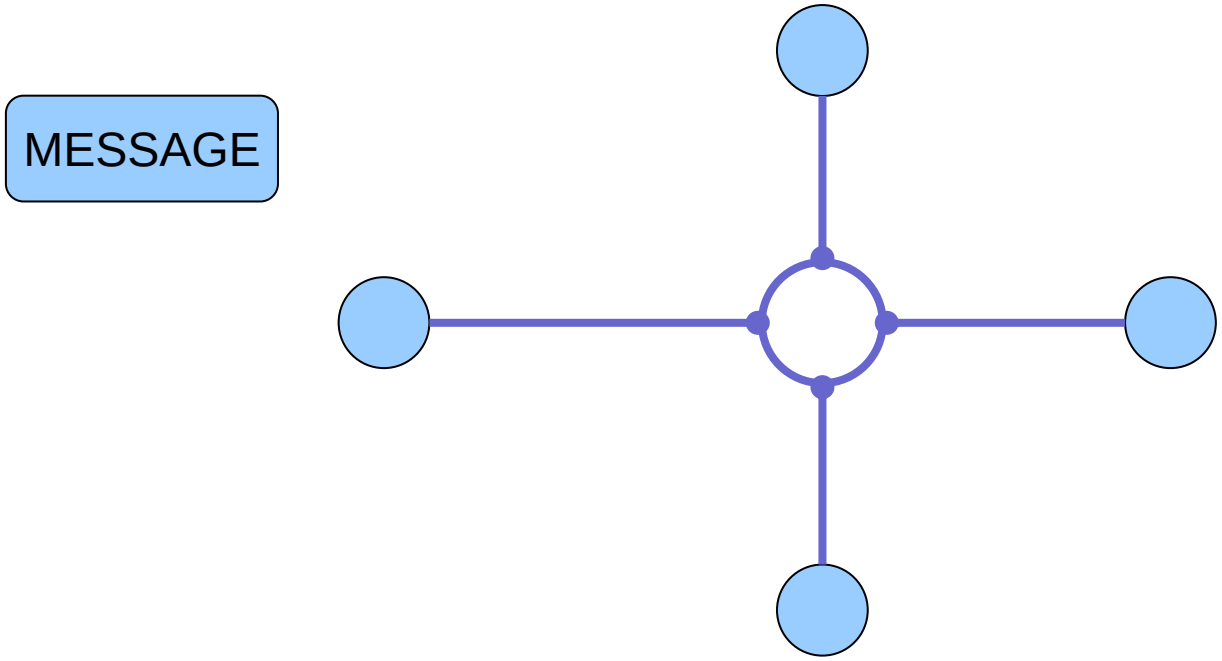
En Etoile

- Dans une **topologie en étoile**, les ordinateurs du réseau sont reliés à un système matériel central appelé **concentrateur** (hub)



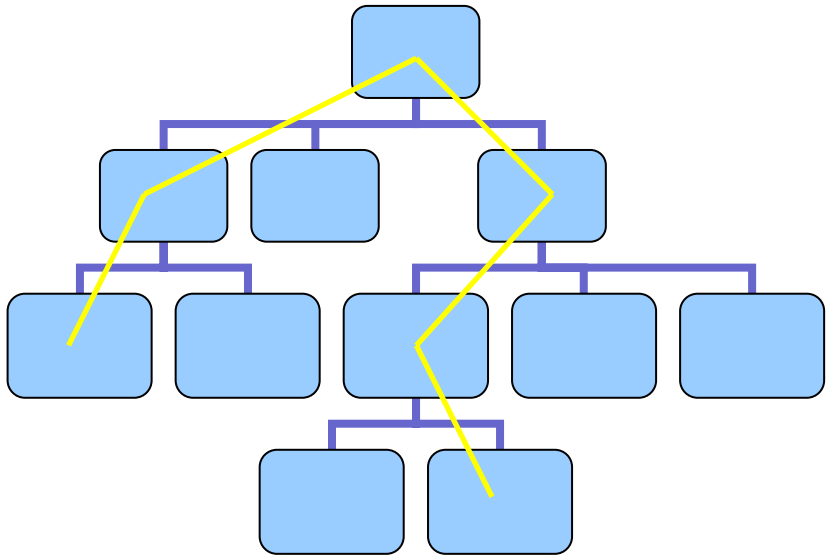
En anneau

- Dans un réseau possédant une **topologie en anneau**, les ordinateurs sont situés sur une boucle et communiquent chacun à leur tour. En réalité, les ordinateurs ne sont pas reliés en boucle, mais à un **répartiteur** qui va gérer la communication entre les ordinateurs qui lui sont reliés en impartissant à chacun d'entres-eux un temps de parole.



Hiérarchiques

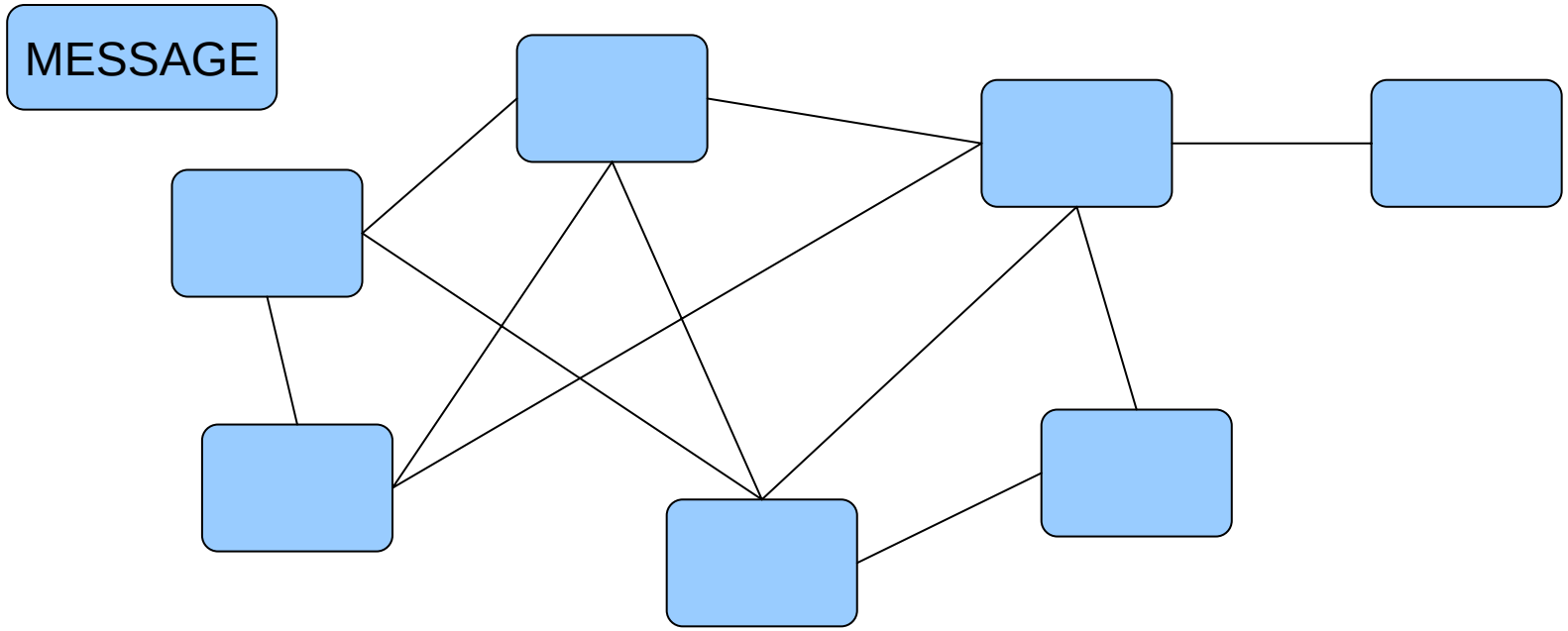
MESSAGE



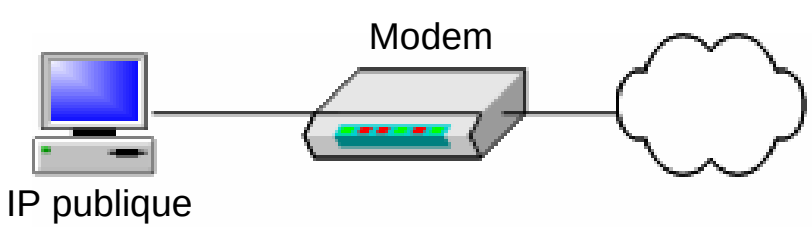
Maillés

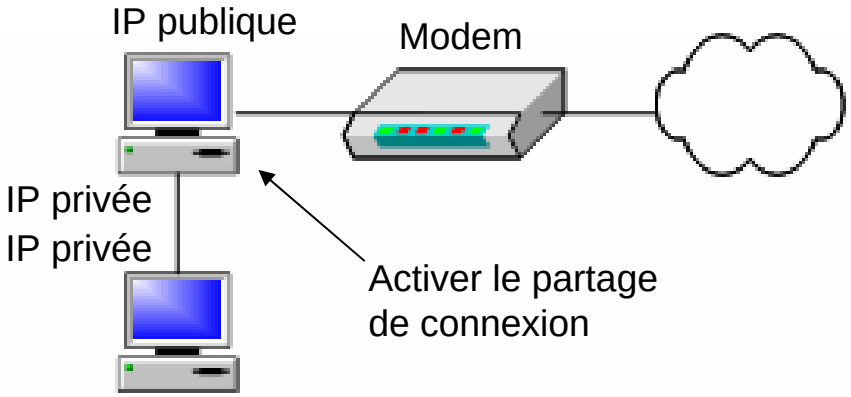
- Une topologie maillée correspond à plusieurs liaisons point à point. Le nombre de liaison est égal à : $\frac{N(N-1)}{2}$

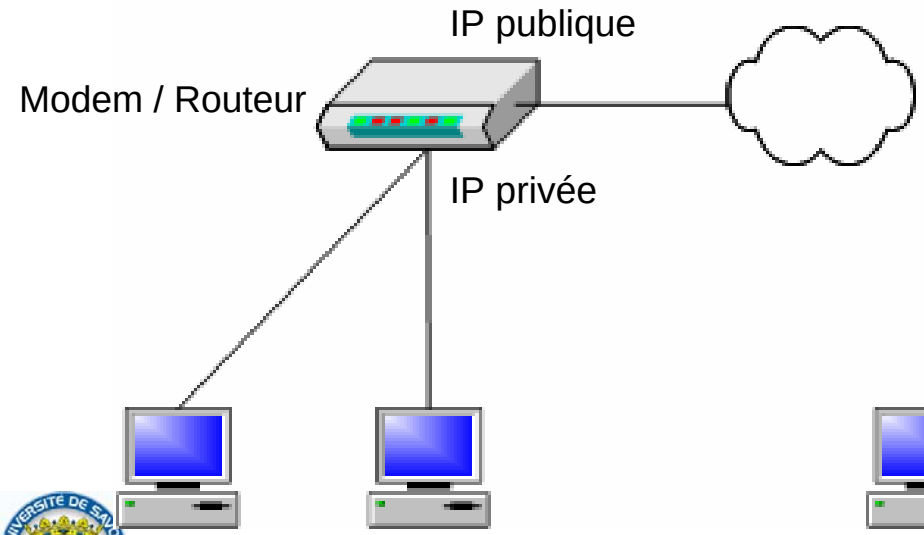
- Cette topologie se rencontre dans les grands réseaux de distribution (Exemple : Internet).

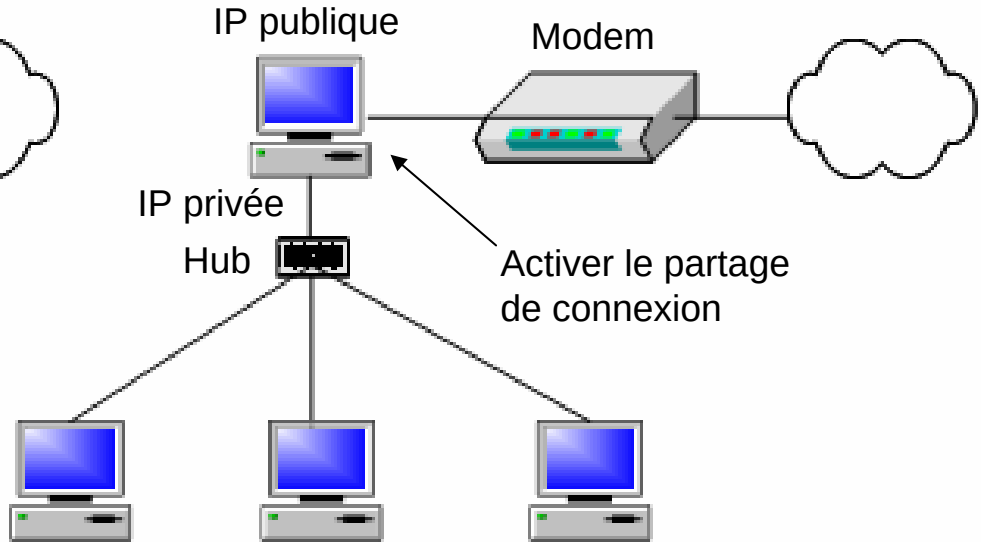


Exemples de réseaux familiaux









Chapitre 1 : Topologie et classification des réseaux

- 1.1 Classification des réseaux : LAN, WAN…
- 1.2 Les supports de transmission
- 1.3 Topologie des réseaux
- 1.4 Caractéristique d'une transmission
- 1.5 Caractéristique des signaux

Sens des échanges

- Full duplex

  Echange bidirectionnel en même temps

- Half duplex

  Echange bidirectionnel mais alternativement

- Simplex :

  Echange unidirectionnel

=>Donner un exemple d'application pour chacun.

La commutation

- Un réseau est constitué de plusieurs nœuds interconnectés par des lignes de communication. Il existe plusieurs méthodes permettant de transférer une données d'un nœud émetteur à un nœud dit récepteur :
  - **La commutation de circuits**
  - **La commutation de paquets**

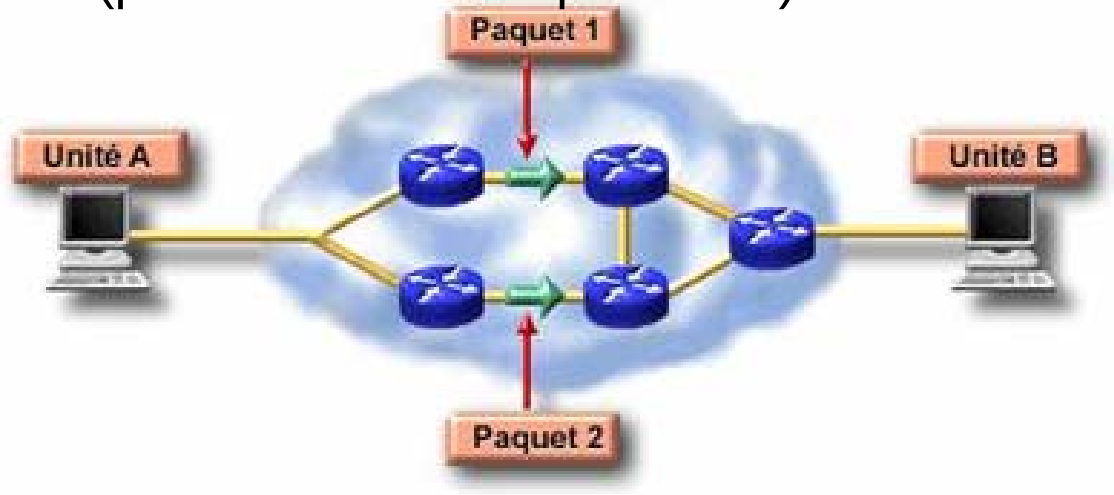
La commutation de circuits

- La **commutation de circuit** est une méthode de transfert de données consistant à établir un **circuit dédié** au sein d'un réseau. La ligne est libéré seulement à la fin de la transmission.

- Il s'agit notamment de la méthode utilisée dans le **réseau téléphonique commuté** (**RTC)**. Le **lien physique** est **maintenu** jusqu'à la fin de l'appel et ne peut être perturbé (tonalité « occupé »)

La commutation de paquets

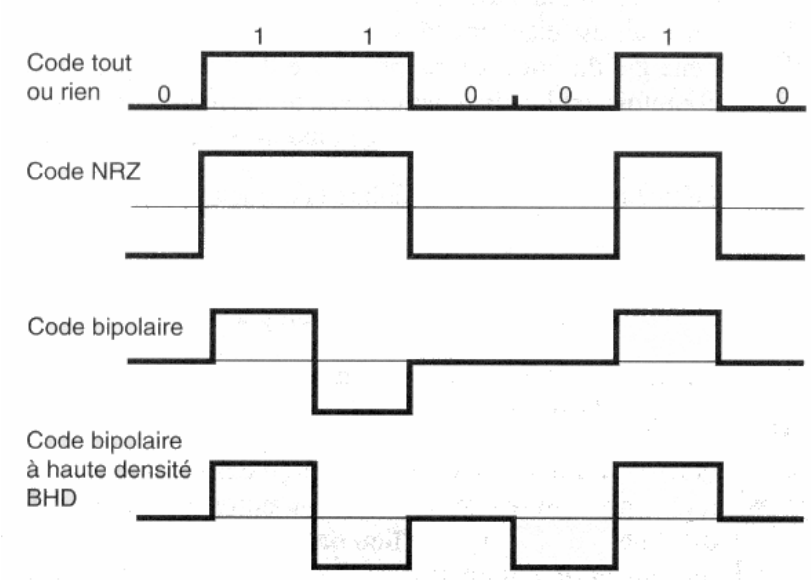
- Lors d'une transmission de données par commutation de paquets (packet switching), les données à transmettre sont découpées en paquets de données (on parle de segmentation) et émis indépendamment sur le réseau.
- Les nœuds du réseau sont libres de déterminer la route de chaque paquet individuellement. Les paquets ainsi émis peuvent emprunter des routes différentes et sont réassemblés à l'arrivée par le nœud destinataire. Il s'agit du mode de transfert utilisé sur internet, car il comporte les avantages d'être très tolérant aux pannes des nœuds intermédiaires (plusieurs chemins possibles).

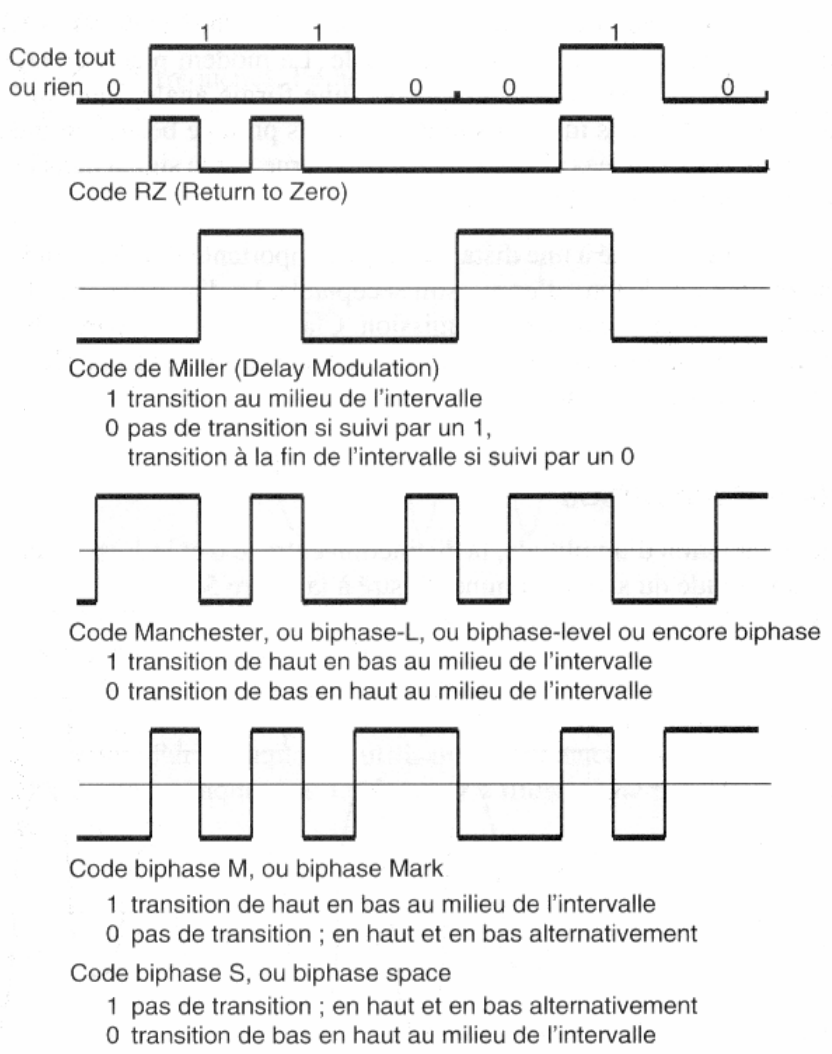


Chapitre 1 : Topologie et classification des réseaux

- 1.1 Classification des réseaux : LAN, WAN…
- 1.2 Les supports de transmission
- 1.3 Topologie des réseaux
- 1.4 Caractéristique d'une transmission
- 1.5 Caractéristique des signaux

Codage en bande de base

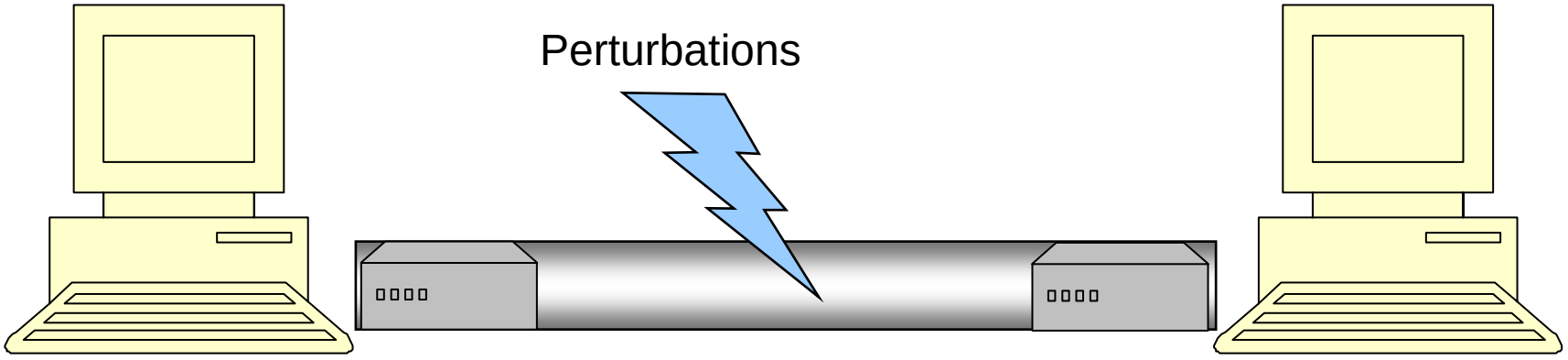




Inconvénients

- Monopolisation du support
- Dispersion du spectre (étalement du signal)
- Sensibilité aux perturbations

Communication : cadre général



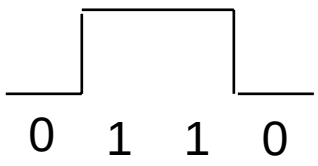
DTE = Data Terminal Equipment

DCE = Data Communication Equipment

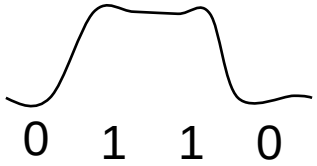
Nature des Informations

Canal de Transmission

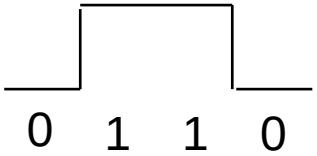
DTE 1 DCE 1 DCE 2 DTE 2



Numérique



Analogique



Numérique

Transmission en bande transposée

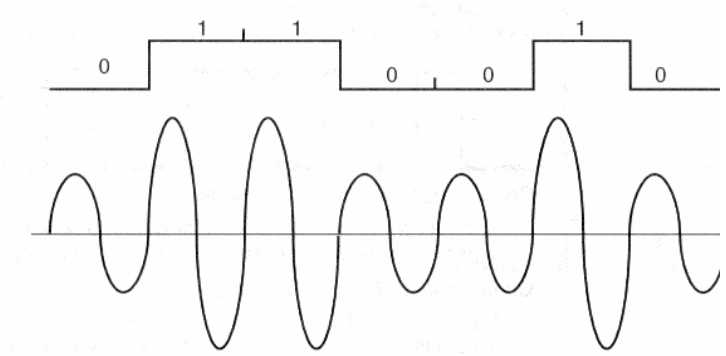
- Circulation des informations sous la forme de modulation d'une onde (analogique):

$$a(t) = A.\sin(\omega t + \varphi)$$

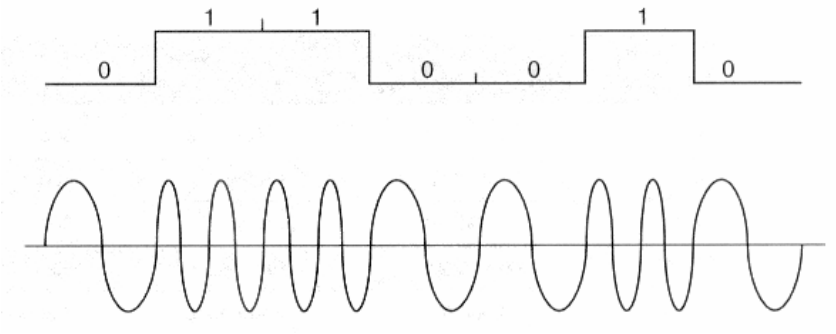
- Le codage peut agir sur:
  - *A: modulation d'amplitude.*
  - *ω: modulation de fréquence.*
  - *φ: modulation de phase .*
  - *Ou une de leur combinaison.*

Codage en large bande

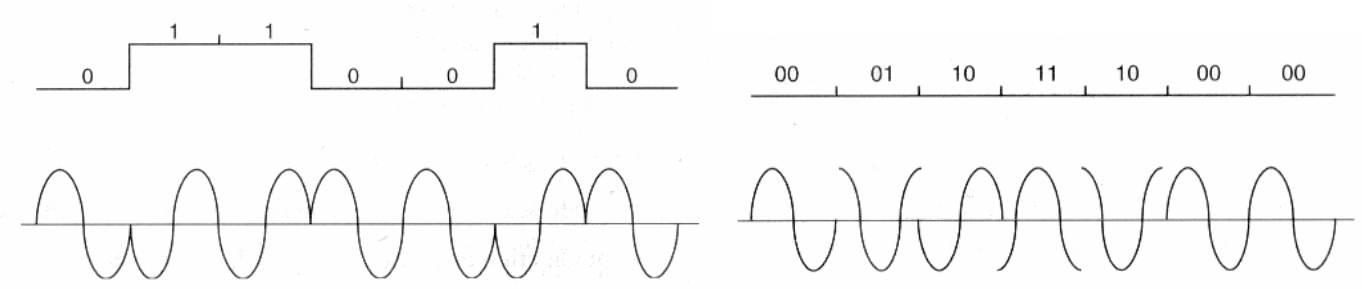
- **Modulation d'amplitude:**



- **Modulation de fréquence:**

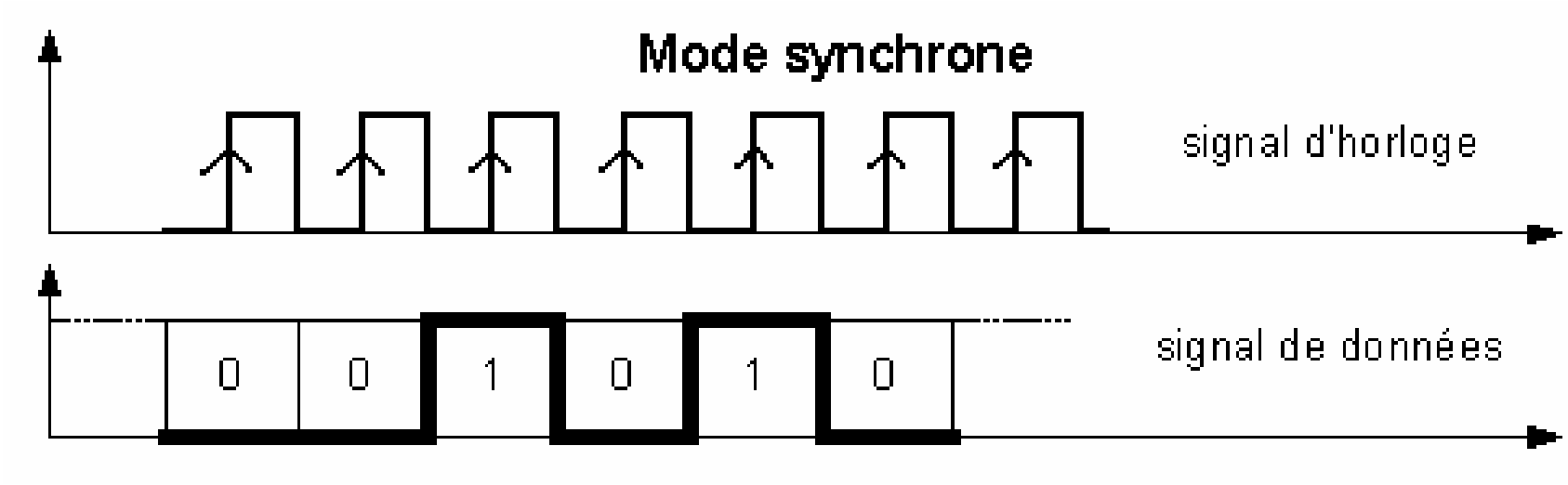


- **Modulation de phase:**



Transmission synchrone

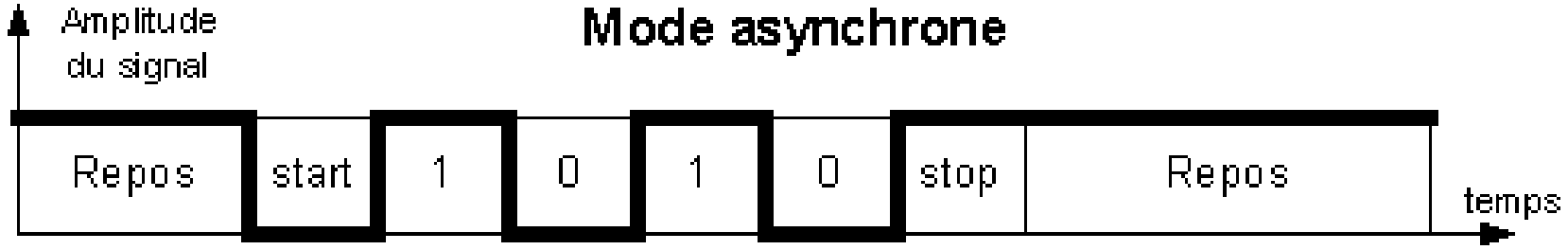
- L’émetteur et le récepteur sont cadencés à la même fréquence d’horloge.
- Le récepteur reçoit de façon continue (même lorsque aucun bit n'est transmis) les informations au rythme où l'émetteur les envoie.



Transmission asynchrone

- L’horloge du récepteur est indépendant de celle de l’émetteur donc pas parfaitement synchrone.

- Le récepteur découvre le début de transmission d'un octet au moment de la réception d'un premier bit appelé "bit de start". Il va ensuite supposer que son horloge à lui est proche de celle de l'émetteur et décoder le reste de l'octet qui arrive. La séquence binaire doit donc être relativement courte.



Exemple : liaison asynchrone

- Une source à une horloge de 1kHz (débit de 1K bit/s). On considère sa fréquence exacte.
- Le récepteur possède donc la même fréquence, en revenche sa stabilité est de 1%.

- Pour lire correctement un bit, la dérive ne doit pas dépasser 10% de la période d'horloge.

>>>Quel est le nombre de bit maximum que l'on peut émettre dans une même trame?

Vrai ou faux ?

- Dans une liaison asynchrone :
  - Le temps d'émission entre deux caractères est fixe?
  - L'émetteur et le récepteur doivent toujours être parfaitement synchronisés?
  - Le débit est en général supérieur que si on utilise une transmission synchrone?

Chapitre 2 : Le modèle OSI de l'ISO

- 2.1 Définition du modèle
- 2.2 Modèle simplifié TCP/IP

Protocole (1)

- Si les **hommes** communiquent entre eux grâce aux différentes **langues**, les **ordinateurs** utilisent différents **protocoles**.

- Pour **transférer** une **information** à un **destinataire** distant, il faut **formater** cette information pour la rendre **compréhensible**, préciser **l'adresse** du destinataire, **établir** le chemin de transmission...

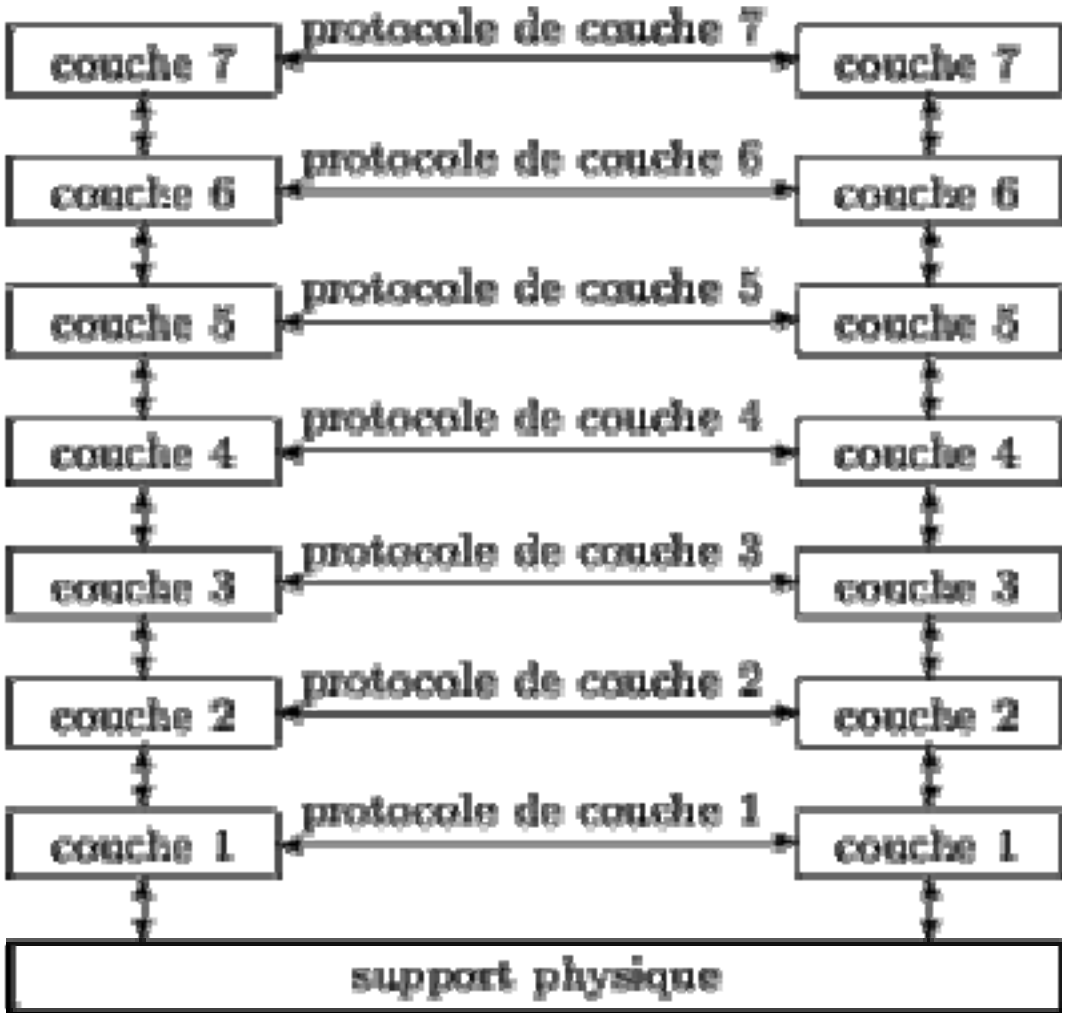
Protocole (2)

- Supposons que quelqu'un veuille **envoyer une lettre** à un destinataire.
  - On va placer cette lettre dans une enveloppe et on note l'adresse.
  - Pour l'acheminement du courrier, le contenu de la lettre n'est d'aucune utilité. Les différents services de la poste regardent les différents champs de l'adresse et dirigent l'enveloppe (donc son contenu) dans la bonne direction.

- Supposons que l'on souhaite **envoyer des données** à un autre ordinateur.
  - On va placer ces données dans une trame et mettre l'adresse.
  - Pour l'acheminement de la trame, les données n'ont aucune utilité. Les données sont enfermées (on dit encapsulées) dans une enveloppe qui contient les informations permettant l'acheminement des données.

- Un protocole, c'est la façon dont la trame (l'enveloppe) est organisée. Le fait de mettre l'adresse de l'ordinateur (« le nom, puis la rue et la ville »). **C'est donc une description formelle de règles et de conventions à suivre dans un échange d'informations.**

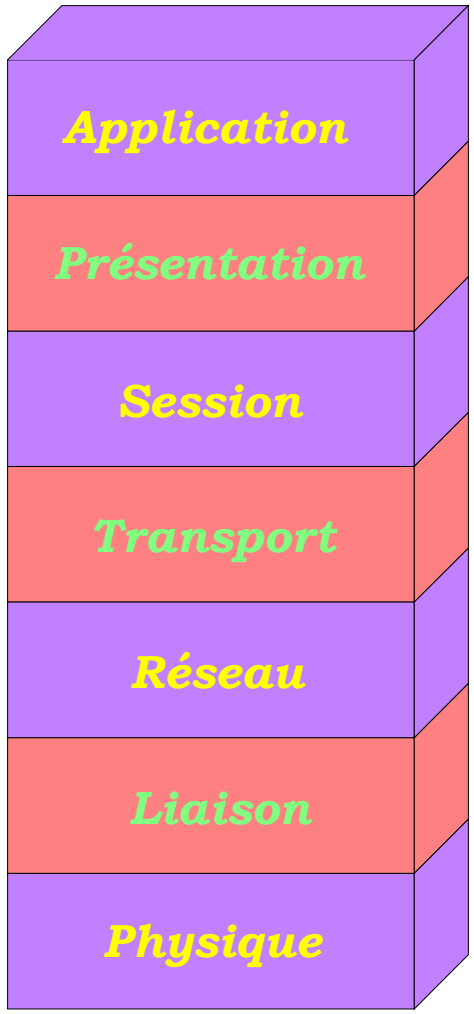
Protocole et modèle OSI



Le Modèle OSI de l'ISO

- **L'International Organization for Standardization (ISO)** a défini un modèle de base appelé **modèle OSI.**

- **Ce modèle** définit **7 niveaux (couches)** différents pour le **transfert de données.**



Le Modèle OSI de l'ISO

- Chaque couche rend service à la couche située au-dessus (émission) ou au dessous (réception).
- **Les couches basses** s'intéressent au transport de l'information (niveaux 1, 2, 3 et 4).
- **Les couches hautes** s'intéressent à leur traitement (niveaux 5, 6 et 7).

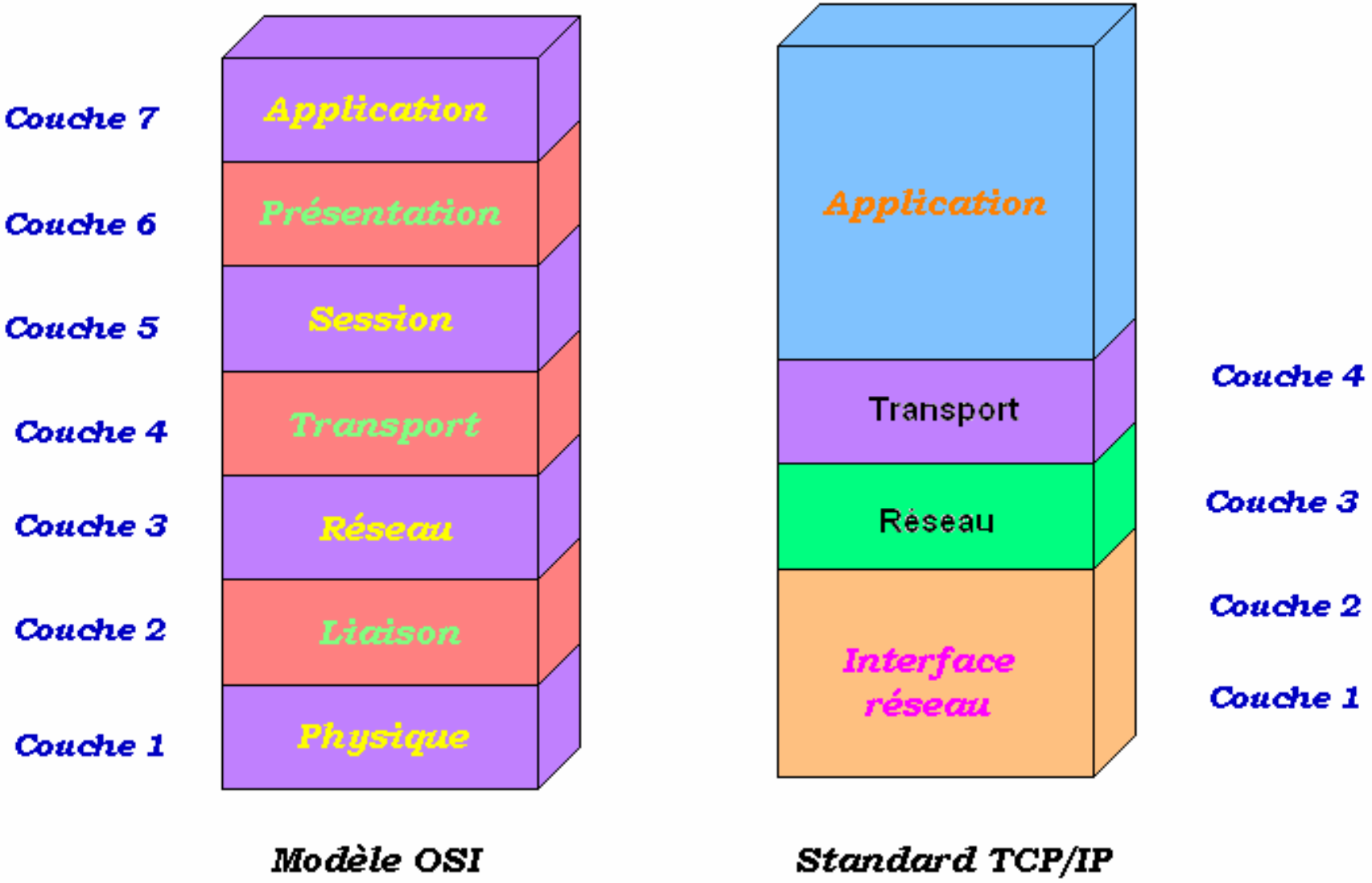
Chapitre 2 : Le modèle OSI de l'ISO

- 2.1 Définition du modèle
- 2.2 Modèle simplifié TCP/IP

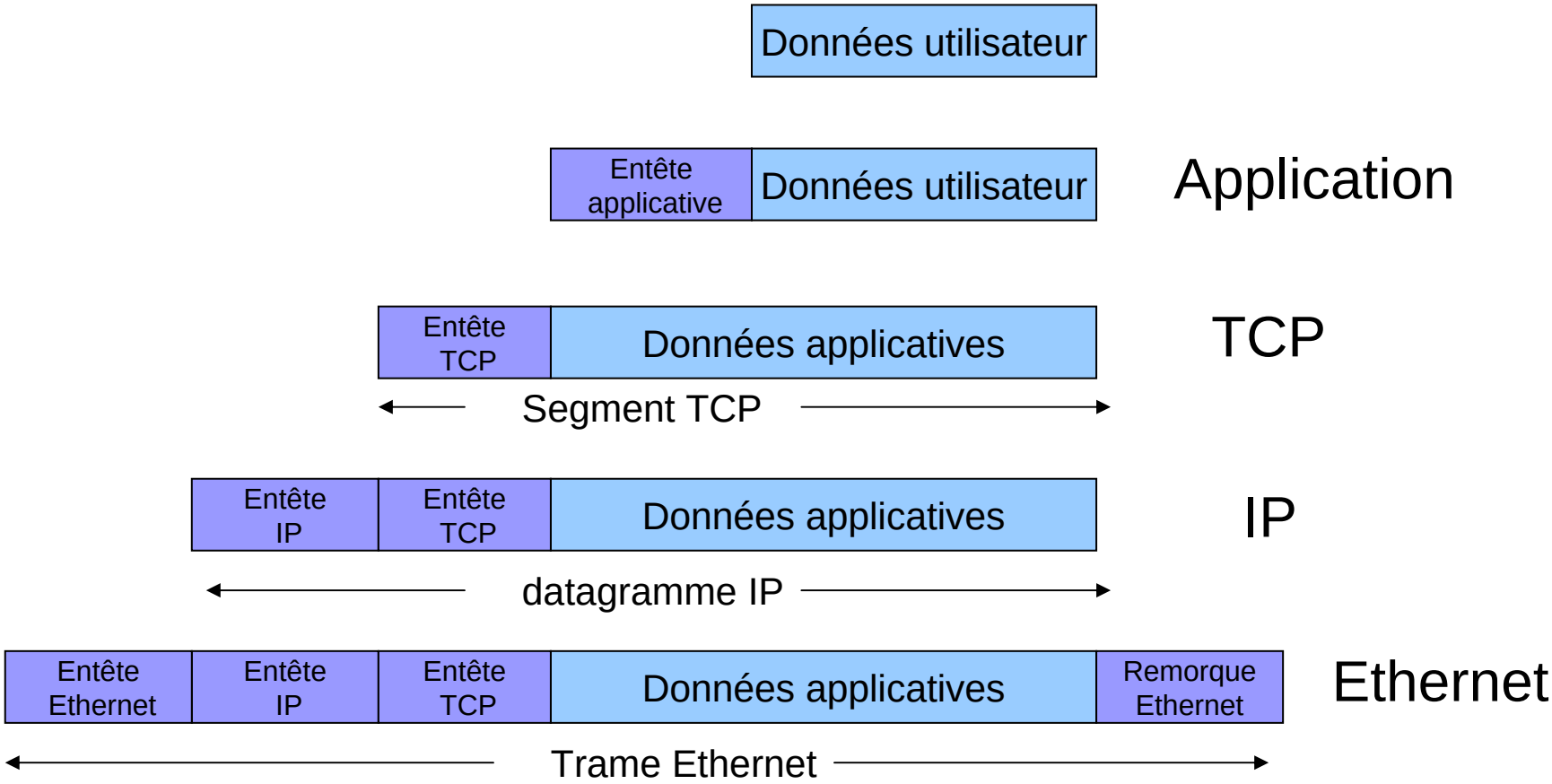
Standard TCP/IP

- Ce standard est structuré en quatre niveaux :
  - **L'interface réseau physique** (couches 1 et 2 du modèle OSI) : dispositifs d'interconnexion et protocole Ethernet.
  - **La couche réseau** (couche 3 du modèle OSI) : acheminer les paquets (routage) d'un ordinateur à un autre.
  - **Le couche transport** (couche 4 du modèle OSI) : Assurer le transport et éventuellement le bon acheminement des paquets.
  - **La couche application** (couches 5, 6 et 7 du modèle OSI) : Protocoles d'applications.

Standard TCP/IP



Encapsulation : exemple



Chapitre 3 : Les éléments d'interconnexion

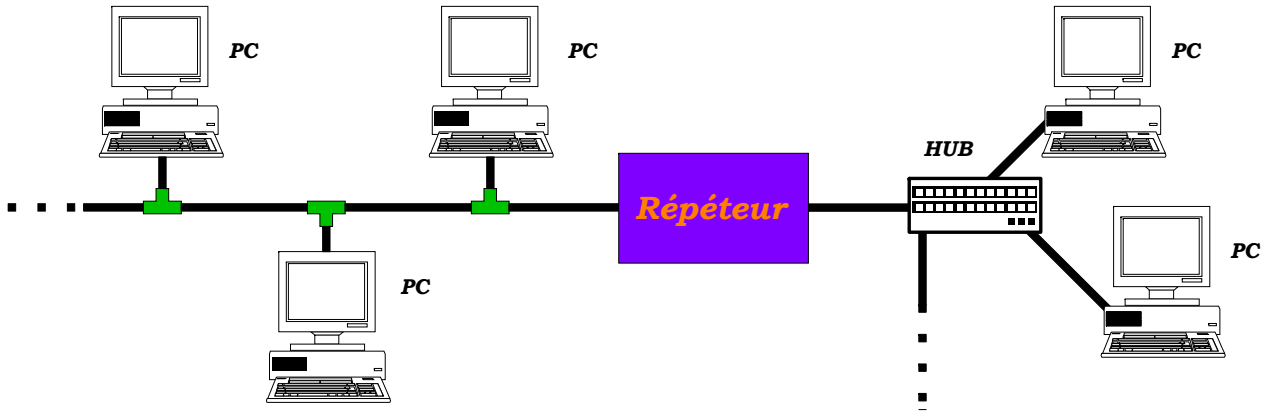
- 3.1 Le répéteur
- 3.2 Le concentrateur (Hub)
- 3.3 Le pont
- 3.4 Le commutateur (Switch)
- 3.5 Le routeur
- 3.6 La passerelle

3.1 Le répéteur

Permet de régénérer le signal d'un même réseau.

Fonctions :

- **Répéter** de bloc d'informations d'un segment à l'autre.
- **Régénérer** du signal pour compenser l'affaiblissement.
- **Changer** de support de transmission (passer d'un câble coaxial à une paire torsadée).

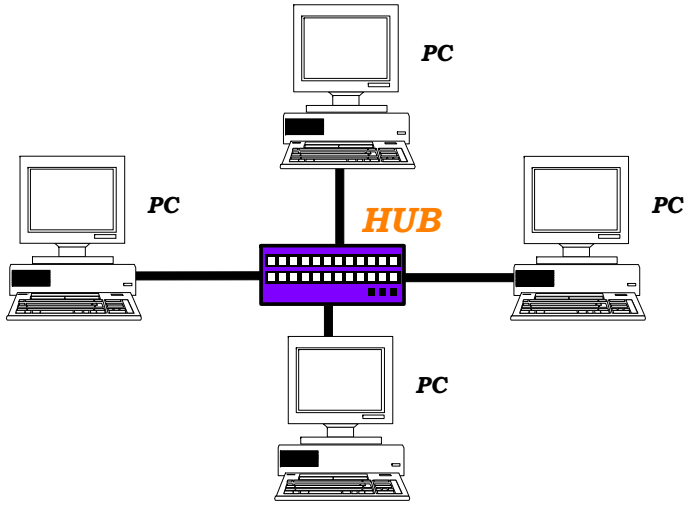


3.2 le concentrateur (Hub partagé)

Permet de connecter plusieurs hôtes entre elles . Il s'agit en fait d'un répéteur multiports

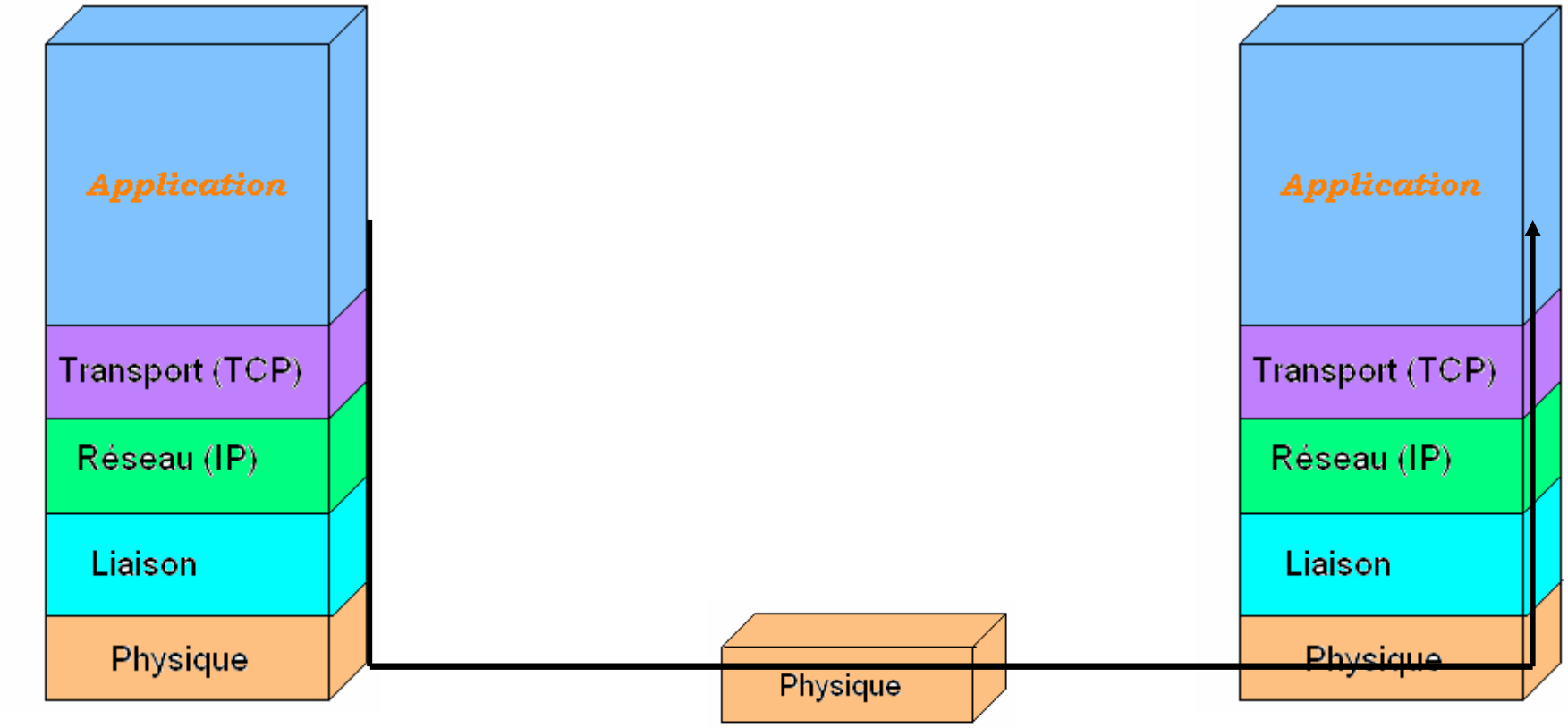
Fonctions :

- **Répéter** de bloc d'informations d'un segment à l'autre.
- **Régénérer** du signal pour compenser l'affaiblissement.
- **Concentrer** plusieurs lignes en une seule.
- Avoir **l'inconvénient** de partager le débit du réseau concerné.



Hub 8 ports

Le répéteur & le Hub



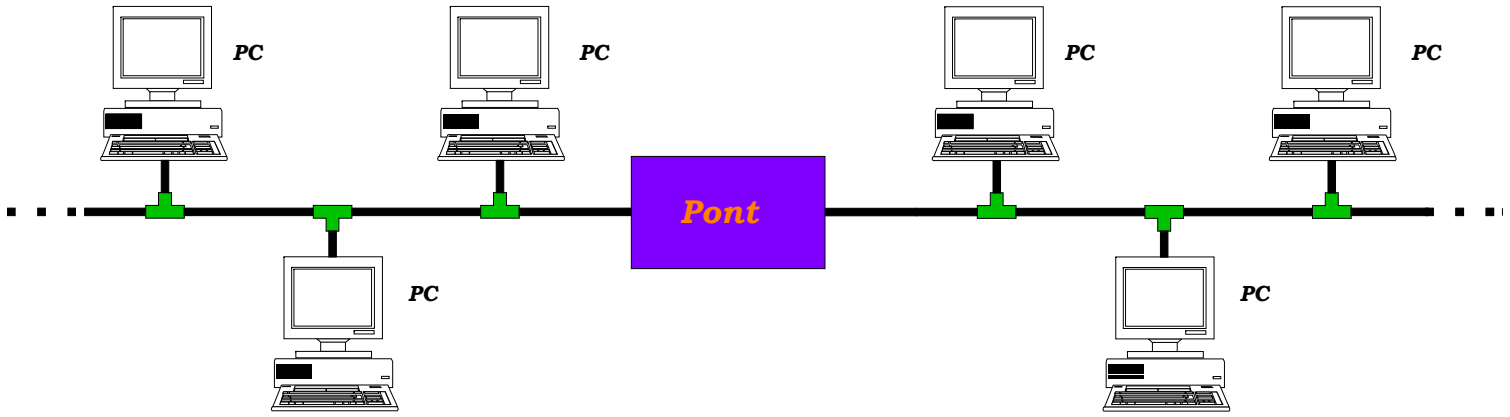
3.3 Le pont

Permet de relier deux réseaux locaux de même type

Fonctions :

- **Reconnaître** les adresses des blocs d'informations qui transitent sur le support physique.
- **Filtrer** les blocs d'information et de laisser passer les blocs destinés au réseau raccordé.

Il analyse l'entête de niveau 2 avant de répéter



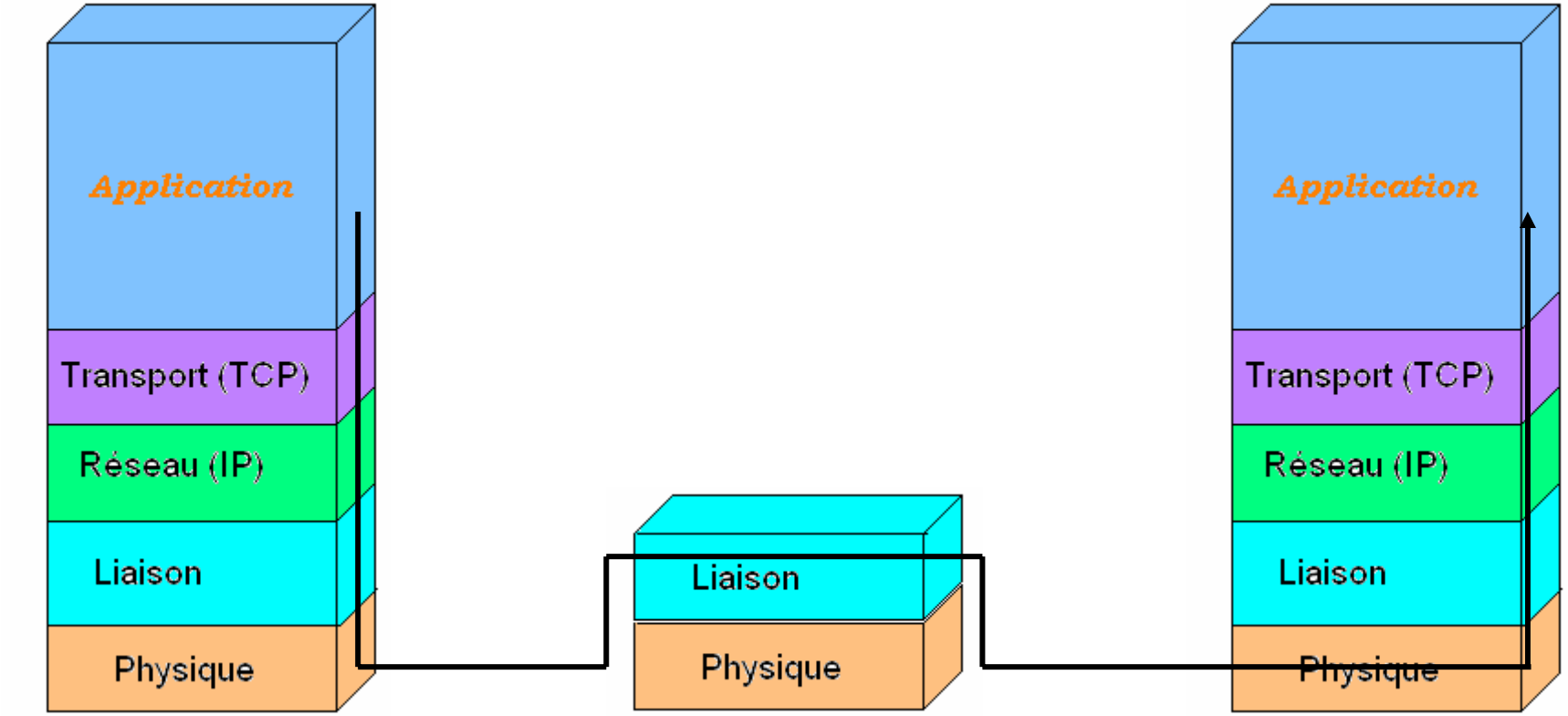
3.4 Les switchs

Similaire aux ponts, sauf qu'ils sont multiports.

- **Fonctions :**
  - **Assurer** l'interconnexion de stations ou de segments d'un LAN en leur attribuant **l'intégralité** de la bande passante. Le débit disponible n'est plus de 10 Mbit/s partagés entre tous les utilisateurs, mais de 10 Mbit/s pour chaque utilisateur.

Il analyse l'entête de niveau 2 avant de répéter

Les ponts & les switch

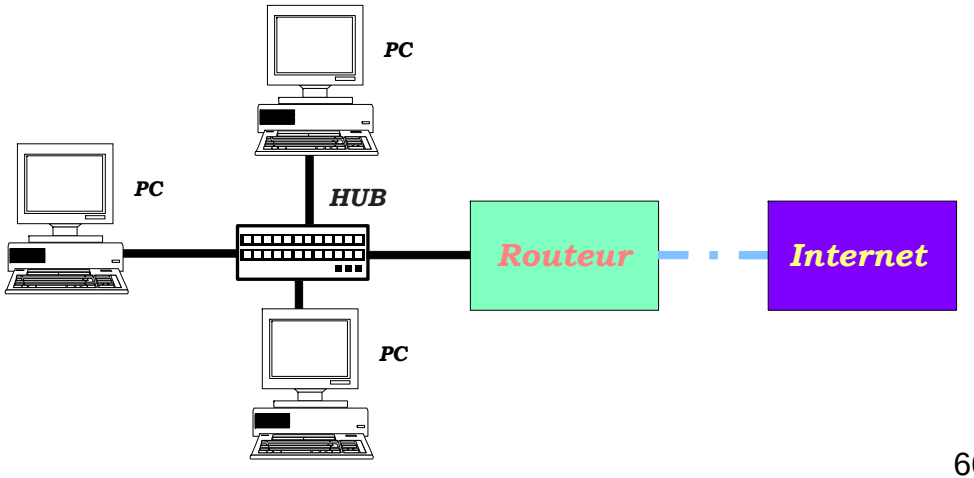


3.5 Les routeurs

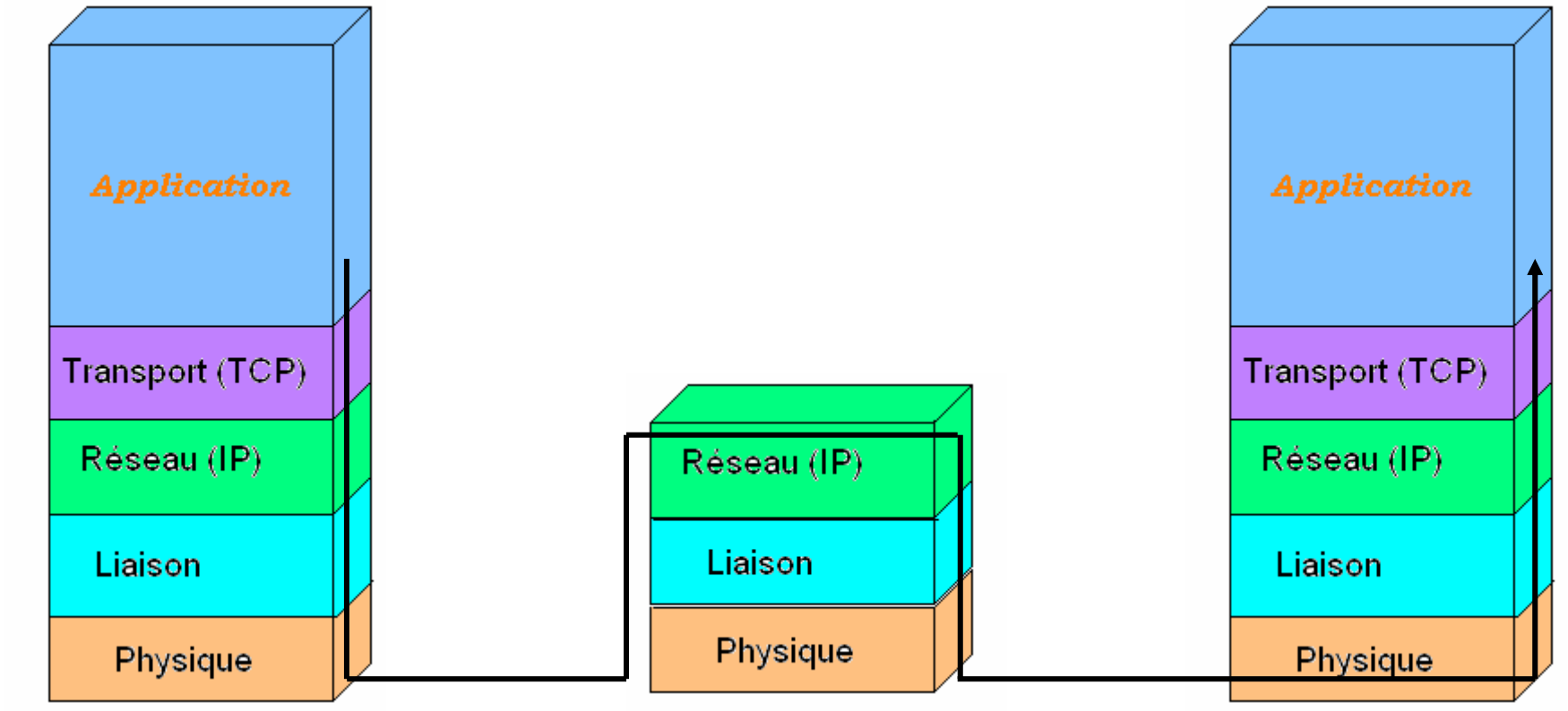
Permet de relier de nombreux réseaux locaux de telles façon à permettre la circulation de données d'un réseau à un autre de la façon optimale

Fonctions :

- **Manipuler** des adresses logiques et non physiques.
- **Permettre** un filtrage très fin des échanges entre les machines (listes de contrôle d'accès).
- **Analyser** et de **choisir** le meilleur chemin à travers le réseau pour véhiculer les blocs d'informations.



Les routeurs



3.6 Les passerelles (Gateway)

Permet de relier des réseaux utilisant des protocoles différents

Fonctions :

- Lorsqu'un utilisateur distant contacte un tel dispositif, ce dernier examine sa requête et, si jamais celle-ci correspond aux règles que l'administrateur réseau a définies, la passerelle crée une liaison entre les deux réseaux. Les informations ne sont donc pas directement transmises, mais traduites afin d'assurer la continuité des deux protocoles.

- Elles fonctionnent au niveau applicatif. Exemple : Relier un LAN à Internet

Chapitre 4 : Couche 2, le protocole Ethernet

- 4.1 Présentation du protocole Ethernet
- 4.2 La trame Ethernet

Ethernet (1)

- Ethernet est un protocole **de réseau local**.
- Ethernet a été standardisé sous le nom **IEEE 802.3**. C'est maintenant une norme internationale.
- On distingue différentes variantes de technologies Ethernet suivant le type et le diamètre des câbles utilisés.

Ethernet (2)

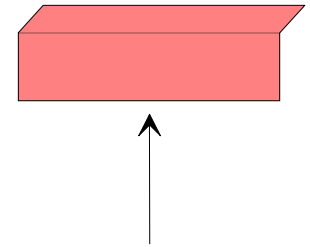
Sigle	Dénomination	Câble	Débit	Portée
10Base-T	Ethernet standard	Paire torsadée (catégorie 3)	10 Mb/s	100m
100Base-TX	Fast Ethernet	Double paire torsadée (catégorie 5)	100 Mb/s	100m
1000Base-T	Ethernet Gigabit	Double paire torsadée (catégorie 5e)	1000 Mb/s	100m
1000Base-LX	Ethernet Gigabit	Fibre optique mono ou multimode	1000 Mb/s	550m
10GBase-SR	Ethernet 10Gigabit	Fibre optique multimode	10 Gbit/s	500m

Chapitre 4 : Couche 2, le protocole Ethernet

- 4.1 Présentation du protocole Ethernet
- 4.2 La trame Ethernet

La trame Ethernet (1)

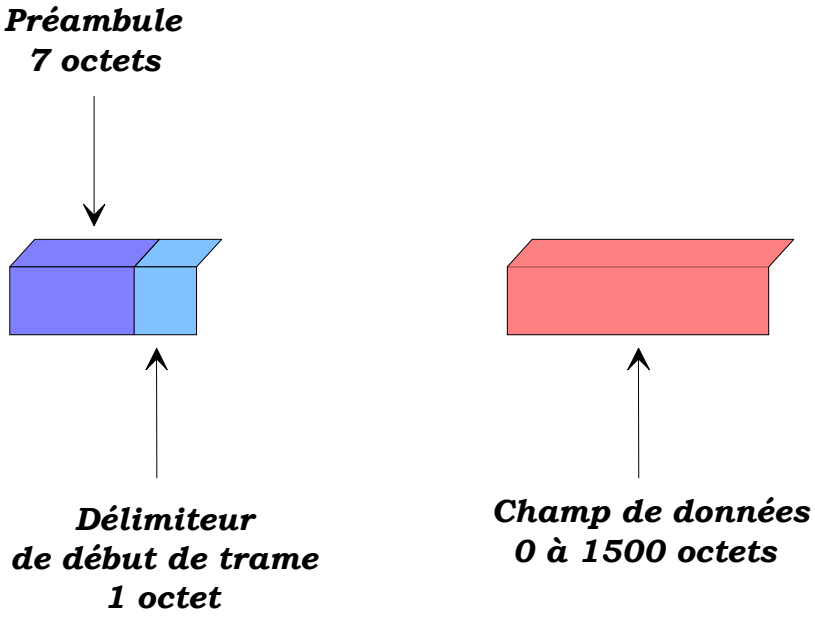
- Les données proviennent de la couche supérieure et seront encapsulées dans la trame Ethernet.



Le préambule

- L'objectif est de **synchroniser** les horloges et de **délimiter** le début de la trame Ethernet. L'entête de la trame contient :
  - Le préambule (7 octets) de valeur 10101010 → synchronisation des horloges
  - la zone de délimitation de début de la trame (1 octet) égale à 10101011

La trame Ethernet (2)

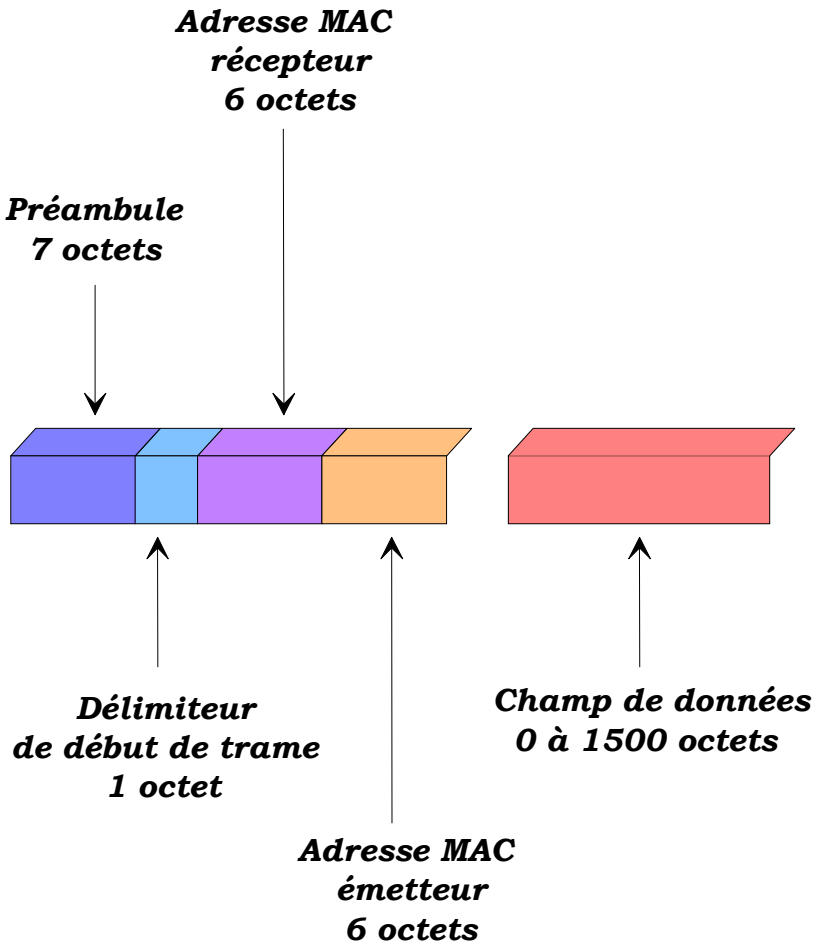


L’adresse Ethernet

- On l’appelle aussi **adresse physique** ou **adresse MAC**, elle est non modifiable.

- Chaque carte Ethernet a une **adresse unique sur 6 octets**, inscrite en usine, faite de **deux parties**:
  - Le **numéro du constructeur** : 3 premier octets
  - le **numéro de la carte** : 3 derniers octets
  - L’adresse FF:FF:FF:FF:FF:FF est réservée pour le broadcast.

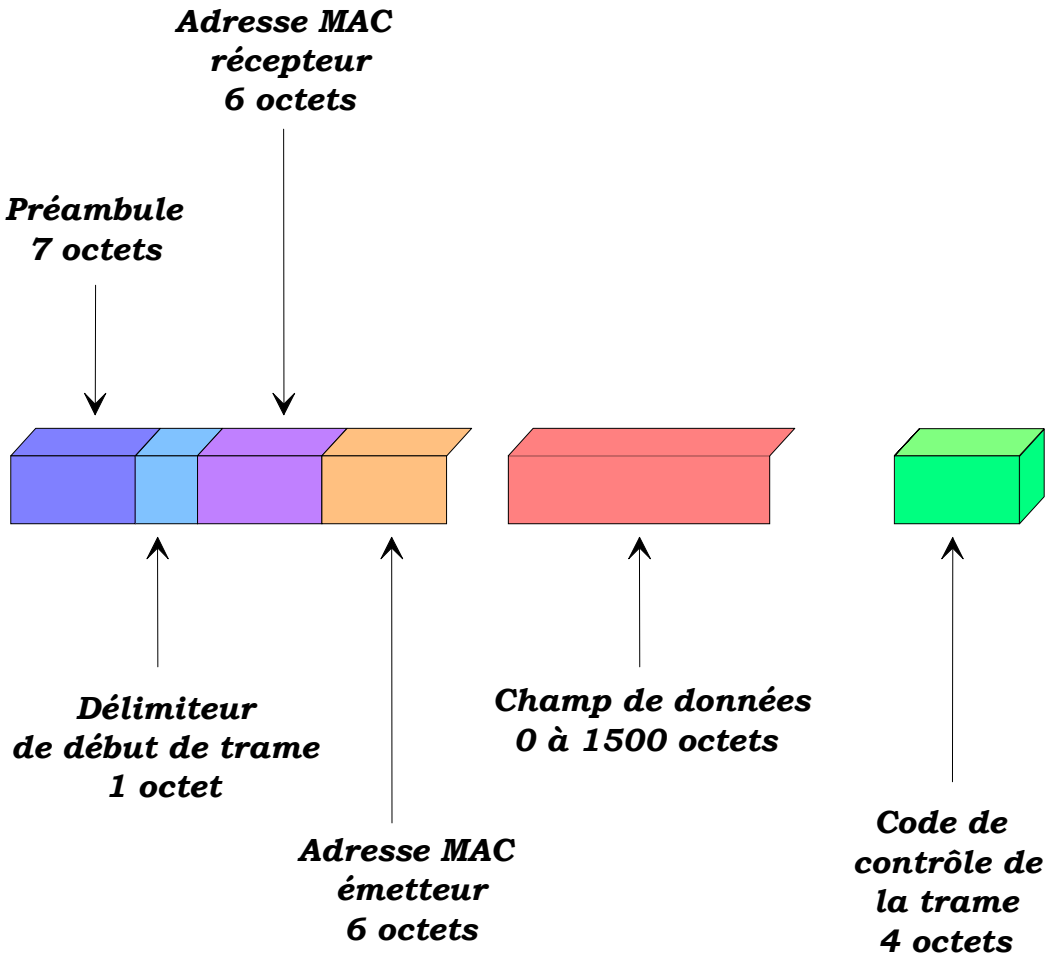
La trame Ethernet (3)



Le contrôle des erreurs

- La fin de trame contient:
  - Le champ de contrôle et de détection d'erreurs étendu sur 4 octets. **(CRC).** Ce champ est recalculé à la réception. Si il y a une différence → erreur transmission

La trame Ethernet (4)



Les collisions (1)

La méthode d'accès sur **Ethernet** est appelée **CSMA/CD** (Carrier Sense Multiple Access / Collision Detection).

- **CS « Carrier Sense »:** Capacité à détecter tout trafic sur le canal (Écouter avant de parler), s'il y a trafic on ne tente pas l'émission.
- **MA « Multiple Access »:** Chaque station a potentiellement accès au canal lorsqu'elle a besoin d'émettre
- **CD « Collision Detect »:** C'est la capacité d'un nœud émetteur à détecter le signal sur le support de transmission.

Les collisions (2)

- Collision !
- DTE2 voit la collision
- DTE1 ne voit rien !

Les collisions (3)

- Afin de pouvoir être sur d'observer une éventuelle collision la norme impose des contraintes.

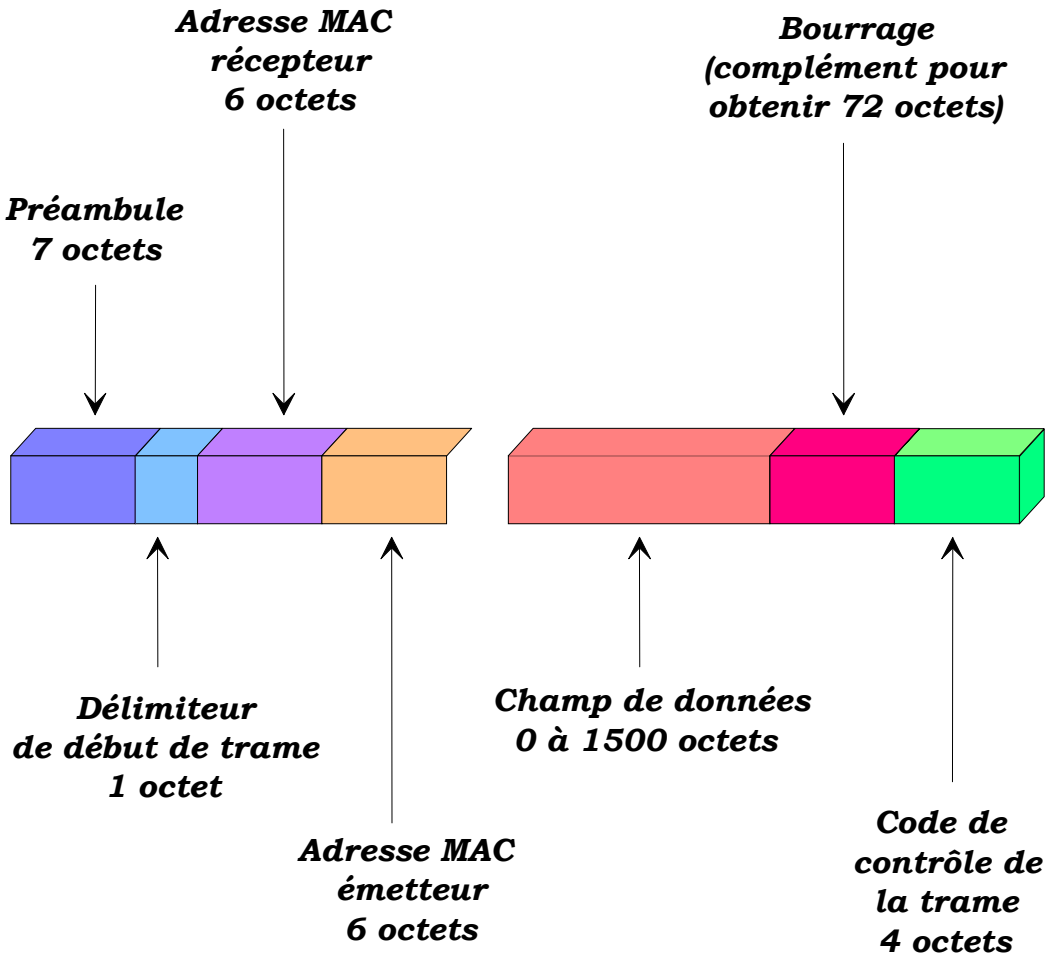
- Dans la norme le temps maximal d'aller retour RTT (round trip time) est fixé à 512 « bit time » (donc dépend du débit du réseau).
  - A 10 Mbit/s, 50 μs correspond à 62,5 octets
  - Afin d'être sur d'émettre plus que le temps maximum d'aller retour (Round Trip Time : RTT), la trame Ethernet à une traille de 72 octets minimum

Les collisions (4)

- 1 trame Ethernet impose au moins 72 octets en étant composée de :
  - 26 octets de protocole (entete Ethernet + CRC)
  - 46 octets de données minimum (pour avoir au moins 72 octets)
  - Si moins de 46 octets à envoyer, on utilise le bourrage (ajout **d'octets**)

Ex : **Requête ARP** = 28 octets + 18 bourrage

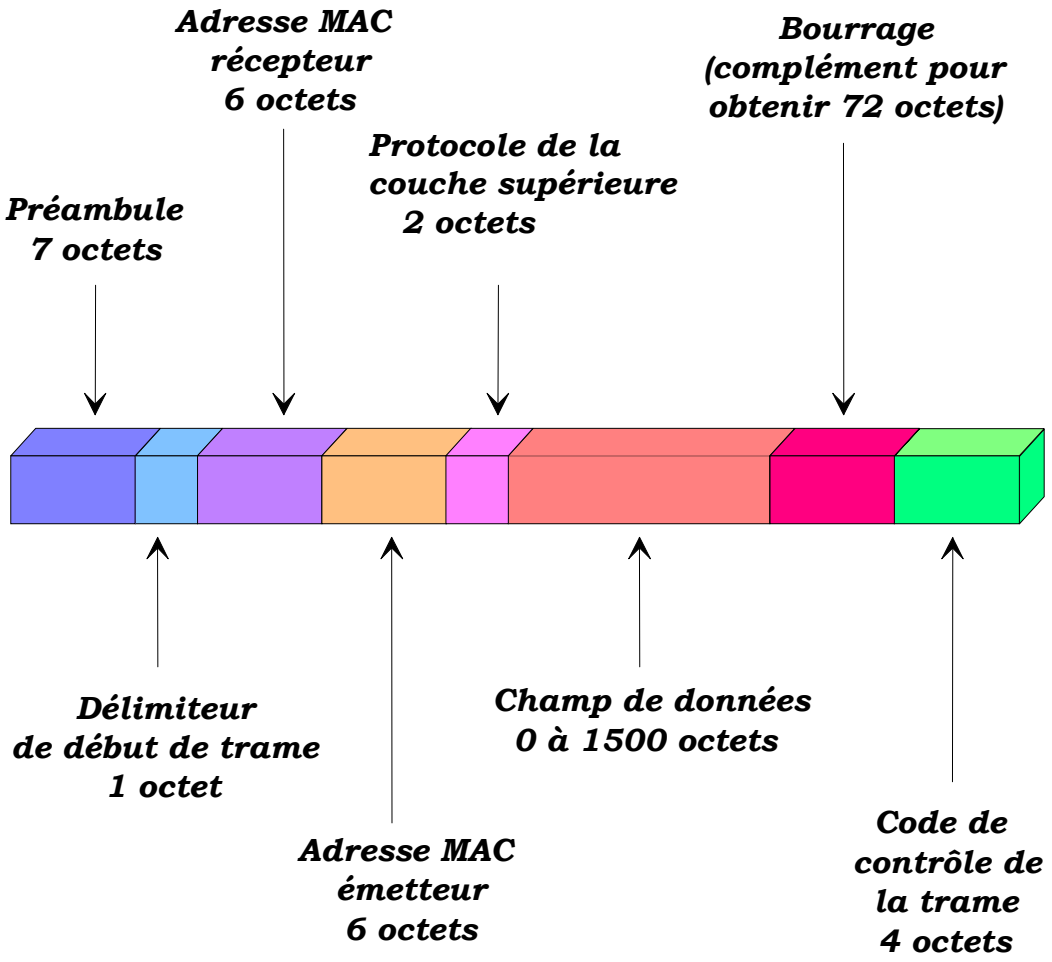
La trame Ethernet (5)



Protocole de niveau 3 (réseau)

- Comment connaître le protocole de la couche supérieur ?
- Le « protocole couche supérieure » permet de définir à quel protocole les données Ethernet doivent être transmises :
  - 0x0800 :**IPv4**
  - 0x86DD :**IPv6**
  - 0x0806 :**ARP**
  - …

La trame Ethernet (6)



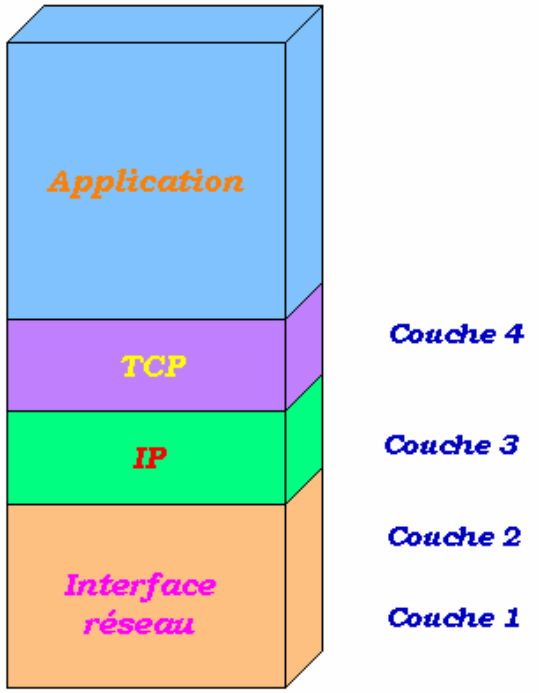
Chapitre 5 : Les protocoles de couche 3 (IP, ARP, ICMP…)

- 5.1 Présentation du protocole IP
- 5.2 Le paquet IP
- 5.3 L'adressage IP
- 5.4 Présentation du protocole ARP
- 5.5 La trame ARP
- 5.6 Présentation du protocole ICMP

Présentation du protocole IP (1)

- Le **protocole IP (Internet Protocole)** est un des protocoles les plus importants d'Internet car il permet l'élaboration et le transport **des paquets IP** (les paquets de données), sans toutefois en assurer la « livraison ».

- En réalité, le protocole IP traite les paquets IP **indépendamment** les uns des autres.



Standard TCP/IP

Présentation du protocole IP (2)

- Le protocole IP a besoin de trois éléments pour transmettre un paquet.
  - **L'adresse IP du destinataire**
  - **Le réseau du destinataire** : Qui est calculé grâce au masque de sous réseau.
  - **La passerelle** : Machine à qui on doit transmettre le paquet si la machine destinatrice n'est pas dans le réseau local.

Chapitre 5 : Les protocoles de couche 3 (IP, ARP, ICMP…)

- 5.1 Présentation du protocole IP
- 5.2 Le paquet IP
- 5.3 L'adressage IP
- 5.4 Présentation du protocole ARP
- 5.5 La trame ARP
- 5.6 Présentation du protocole ICMP

Le paquet IP

- On parle de **paquet IP** ou de **datagramme IP**.
- Le paquet IP ne fait que contenir les informations nécessaires à la réalisation d'une interconnexion.
- Le **champ de données** de la **trame Ethernet** correspond au **paquet IP**.

L’entête IP (1)

<= **32 bits** ==>

Version (4 bits)	**Longueur en-tête** (4 bits)	**Type de service** (8 bits)	**Longueur totale** (16 bits)
Identification (16 bits)		**Drapeaux** (3 bits)	**Décalage fragment (offset)** (13 bits)
Durée de vie (8 bits)	**Protocole supérieur** (8 bits)	**Somme de contrôle en-tête** (16 bits)	
Adresse IP source (32 bits)			
Adresse IP destination (32 bits)			
Données IP			

L’entête IP (2)

- **Version** (4 bits) : Version du protocole IP (IPv4 ou IPv6)
- **Longueur d'en-tête**, ou *IHL* pour *Internet Header Length* (4 bits) : il s'agit du nombre de mots de 32 bits constituant l'en-tête
- **Type de service** (8 bits) : Peu utilisé. Il indique la façon selon laquelle le datagramme doit être traité. (Priorité, délais…)
- **Longueur totale** (16 bits): Il indique la taille totale du datagramme en octets. (< 65536 octets). Utilisé conjointement avec la taille de l'en-tête, ce champ permet de déterminer où sont situées les données.

L’entête IP (3)

- **Identification, drapeaux (flags) et déplacement de fragment** sont des champs qui permettent la fragmentation des datagrammes.

- **Durée de vie** appelée aussi **TTL**, pour *Time To Live* (8 bits) : Ce champ indique le nombre maximal de routeurs à travers lesquels le datagramme peut passer. Ainsi ce champ est décrémenté à chaque passage dans un routeur, lorsque celui-ci atteint la valeur critique de 0, le routeur détruit le datagramme. Cela évite l'encombrement du réseau par les datagrammes perdus. Sa valeur initiale est déterminée par la couche supérieure.

- **Protocole** (8 bits) : Identifie le protocole de la couche supérieure pour transmettre les réceptions de paquets (ex TCP : 6)

L’entête IP (4)

- **Somme de contrôle de l'en-tête** (16 bits) : Ce champ permet de contrôler l'intégrité de l'en-tête afin de déterminer si celui-ci n'a pas été altéré pendant la transmission.
- **Adresse IP source** (32 bits) : Adresse IP de la machine émettrice, il permet au destinataire de répondre.
- **Adresse IP destination** (32 bits) : Adresse IP du destinataire du message.

Chapitre 5 : Les protocoles de couche 3 (IP, ARP, ICMP…)

- 5.1 Présentation du protocole IP
- 5.2 Le paquet IP
- 5.3 L'adressage IP
- 5.4 Présentation du protocole ARP
- 5.5 La trame ARP
- 5.6 Présentation du protocole ICMP

L’adressage IP

- Une **adresse IP**, universelle ou publique, est **unique au niveau mondial**.
- Elle est codée sur **32 bits** soit **4 octets**, la notation la plus courante consiste à indiquer chaque octet en décimal et à les séparer par des points.
  - *Exemple : **193.160.13.245***

- Plus précisément, l’adresse IP d’un ordinateur est composée de deux parties :
  - *La première partie correspond à **l’adresse du réseau.***
  - *La deuxième partie correspond à **l’adresse de la machine** sur le réseau.*

Attribution d’une adresse IP

- L’adresse publique d’ordinateur pour une connexion à Internet est attribuée parmi celles dont dispose votre **Fournisseur d’Accès à Internet (FAI).**

- Celle-ci a été demandée au préalable à un organisme officiel, garantissant ainsi l’unicité des adresses de réseau au niveau mondial. C'est **l'ICANN (Internet Corporation for Assigned Names and Numbers)**, qui est chargée d'attribuer des adresses IP publiques.

Le masque de sous-réseau

- Un **masque** de sous-réseau a la **même forme** qu'une **adresse IP** (32 bits). Il a pour rôle de **distinguer** le **numéro du réseau**, du **numéro de l'ordinateur** dans ce réseau.

- Dés lors qu'un **équipement** possède une **adresse IP**, il est extrêmement important de connaître le masque associé afin de déterminer le réseau dans lequel appartient cette machine.

Structure du masque de sous-réseau

- Par convention, les bits de gauche d'un masque sont à 1 et les bits de droite sont à 0.
  - Exemple : 11111111 11111111 11111111 00000000 ce qui correspond à 255.255.255.0
- Pour connaître le réseau dans lequel appartient une machine, on fait un & logique entre le masque de sous réseau et l'adresse IP de la machine.
- Exemple:

Une machine possède l'adresse IP :	194 . 214 . 110 . 35
Elle possède une masque :	255 . 255 . 255 . 0
L'adresse du réseau est :	194 . 214 . 110 . 0
L'adresse de cette machine dans le réseau est :	35

- Dans chaque réseau, les adresses dont les bits de machine sont tous à 0 (valeur 0) ou tous à 1 (valeur 255) ne peuvent être attribuées :
  - Le nombre 0 désigne le réseau dans son ensemble
  - 255 représente une adresse de diffusion (broadcast) à destination de tous les nœuds du réseau.

L’adressage IP Public

On utilisait auparavant un système de classe afin de répartir les adresse IP. Cette notion est maintenant obsolète et on utilise maintenant l’adresse CIDR (Classless Inter-Domain Routing).

L’adressage IP Privé

- Ces adresses ne sont jamais utilisées sur Internet, car non « routées ». C’est-à-dire qu’aucun paquet d’un ordinateur possédant une adresse privée ne sera transmis aux autres ordinateurs.

- Dans ce cas, choisir de préférence les adresses réservées à l’usage privé :
  - 10.0.0.1 à 10.255.255.254
  - 172.16.0.1 à 172.31.255.254
  - 192.168.0.1 à 192.168.255.254 (les plus courantes)

Limitation du nombre d’adresses disponibles

- Le nombre d’adresse IP est devenu trop faible.

- Solution
  - Utilisation des adresses privées avec partage de la connexion internet.
  - Passer à IPv6

Chapitre 5 : Les protocoles de couche 3 (IP, ARP, ICMP…)

- 5.1 Présentation du protocole IP
- 5.2 Le paquet IP
- 5.3 L'adressage IP
- 5.4 Présentation du protocole ARP
- 5.5 La trame ARP
- 5.6 Présentation du protocole ICMP

Le protocole ARP

- **L'adresse Ethernet** *(MAC)* est une **adresse unique** sur 48 bits *(6 octets)* associée à une carte Ethernet.
- Lorsqu'une machine A *(@EthA, @IPA)* veut émettre un paquet IP vers une machine B *(@IPB)*, A doit connaître l'adresse Ethernet de B *(@EthB)* de façon à construire la trame Ethernet.
- Pour retrouver l’adresse Ethernet à partir de l’adresse IP du récepteur B, l'émetteur A utilise **le protocole ARP** *(Protocole de résolution d’adresse).*

Le protocole ARP

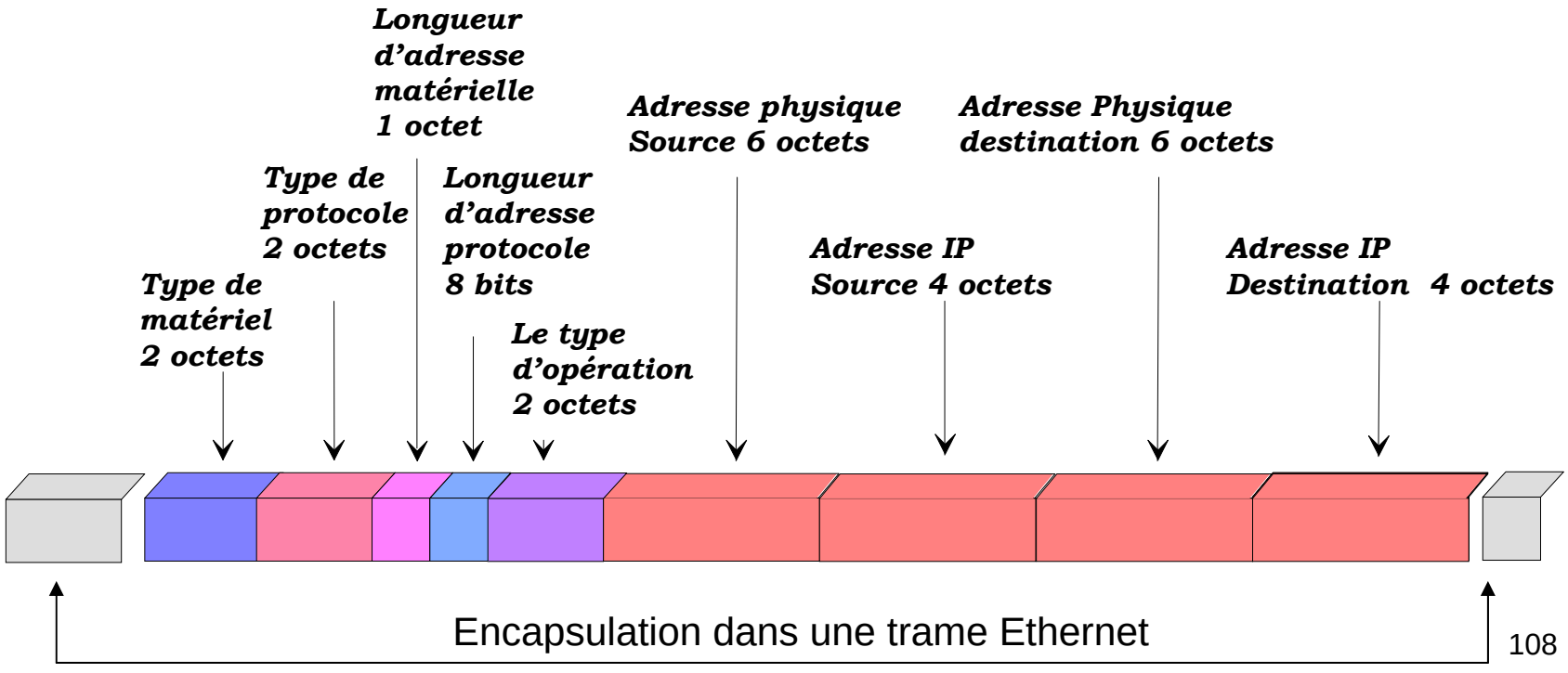
- **Principe:**
  1. L'émetteur A envoie une **trame Ethernet** de diffusion (broadcast) contenant un message ARP « ARP Request » demandant **qui est *@IPB ?***
  2. Toutes les machines du réseau local reçoivent la requête. Seul B d'adresse *@IPB* se reconnaît, et elle répond à A *(@IPA)* dans une trame destinée à *@EthA « ARP Reply »*.
  3. La machine A retrouve l'*@EthB* de la machine B dans la trame Ethernet répondue.
  4. Chaque machine maintient en mémoire une **table ARP de correspondances *@IP / @Eth*** pour éviter trop de requêtes *ARP*. Chaque entrée de la table à une durée de vie limitée.

Chapitre 5 : Les protocoles de couche 3 (IP, ARP, ICMP…)

- 5.1 Présentation du protocole IP
- 5.2 Le paquet IP
- 5.3 L'adressage IP
- 5.4 Présentation du protocole ARP
- 5.5 La trame ARP
- 5.6 Présentation du protocole ICMP

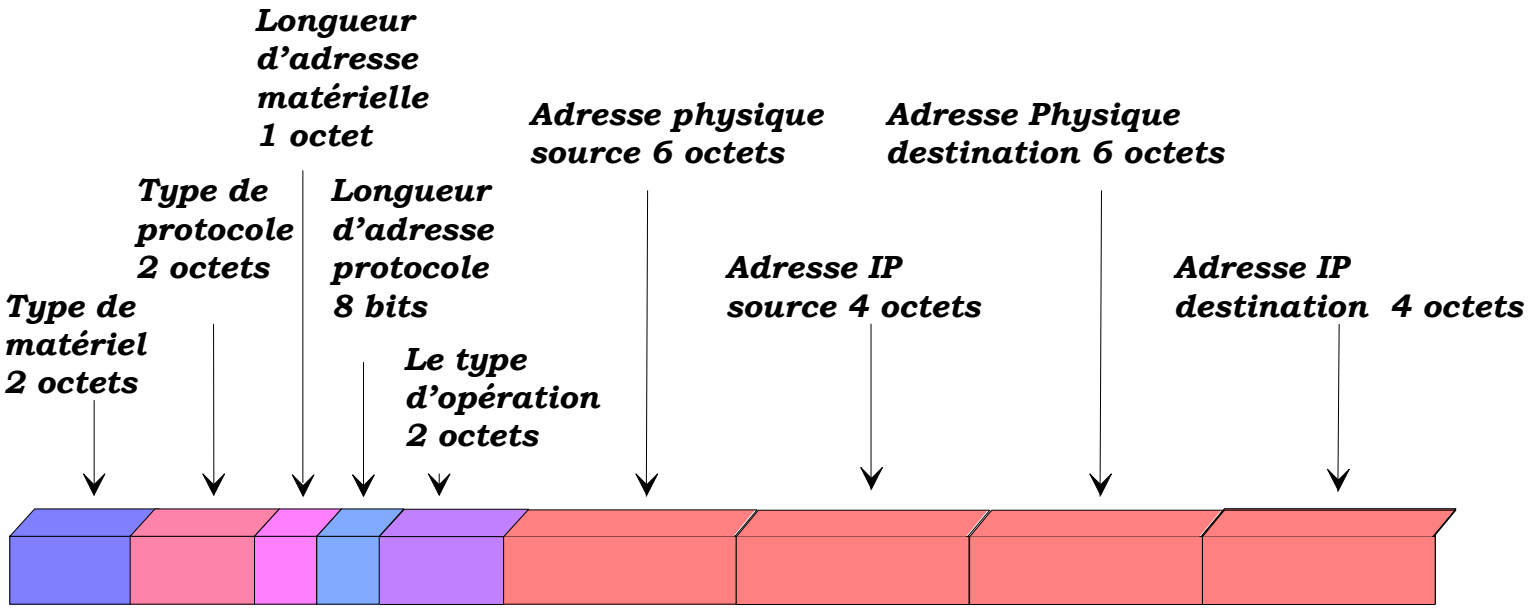
La trame ARP Request

- **Type de matériel :** 0x01(Ethernet)
- **Type de protocole :** 0x0800 (IP)
- **Longueur d'adresse matériel :** Ethernet => 6 octets
- **Longueur d'adresse protocole :** IP => 4 octets
- **Type d'opération :** Request =>0x01 / Reply =>0x02



La trame ARP Reply

- La trame ARP Reply est similaire sauf :
  - Le champ Type d'opération sera « Reply »
  - Le remplissage de l'adresse physique source sera la réponse de « l'ARP request »



Chapitre 5 : Les protocoles de couche 3 (IP, ARP, ICMP…)

- 5.1 Présentation du protocole IP
- 5.2 Le paquet IP
- 5.3 L'adressage IP
- 5.4 Présentation du protocole ARP
- 5.5 La trame ARP
- 5.6 Présentation du protocole ICMP

ICMP : Internet Control Message Protocol

- Le protocole ICMP est un protocole qui permet de gérer les informations relatives aux erreurs des machines connectées. Etant donné le peu de contrôles que le protocole IP réalise, il permet non pas de corriger ces erreurs mais d'en avertir les couches voisines.

- Ainsi, le protocole ICMP est utilisé par tous les routeurs, qui l'utilisent pour signaler une erreur.

La datagramme ICMP

- Bien qu'il soit à un niveau équivalent au protocole IP un paquet ICMP est néanmoins encapsulé dans un datagramme IP.

<table>
<tr><td colspan="3">Entête IP</td></tr>
<tr><td>Type de message</td><td>Code</td><td>Somme de contrôle</td></tr>
<tr><td colspan="3">Bourrage ou données</td></tr>
<tr><td colspan="3">Données (optionnel et de longueur variable)</td></tr>
</table>

Type et Code

- Les champs Type et Code sont codés respectivement sur 8 bits ce qui donne un totale de 2 octets. Ils représentent la définition de message d'erreur contenu. La combinaison la plus connue est :
  - Type : 8, Code : 0 correspondant à une demande d’écho (PING)
  - Type : 0 : Code : 8 correspond à une réponse à une demande d’écho

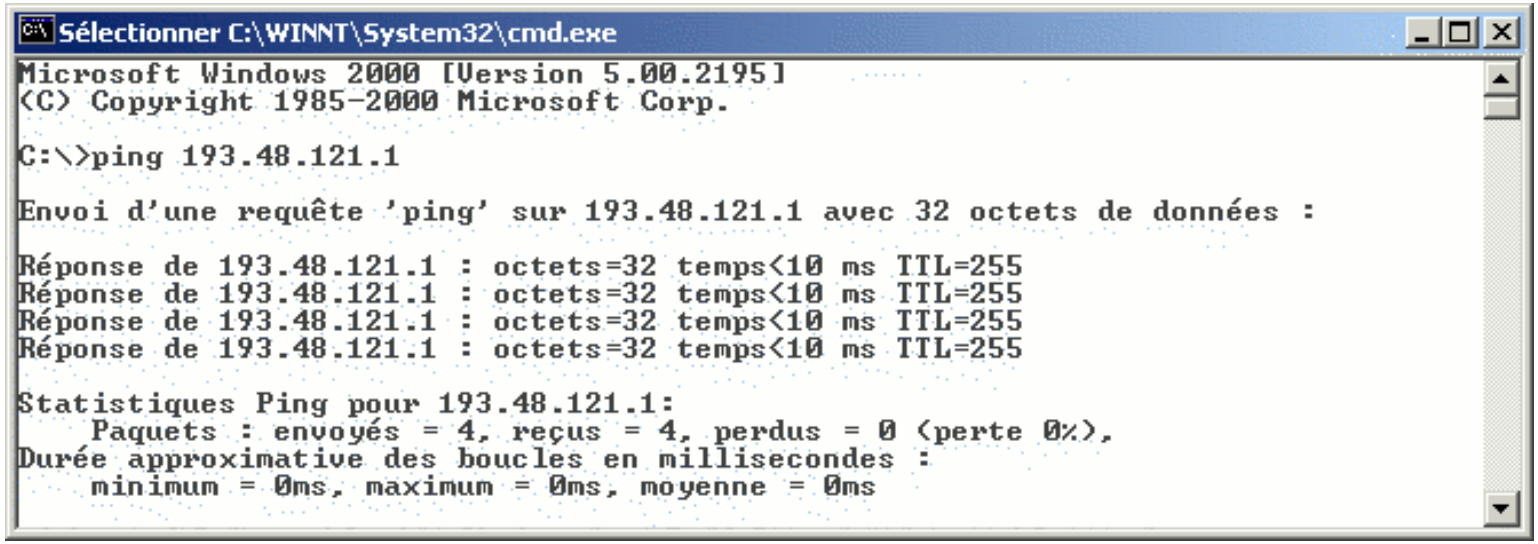
La commande PING (1)

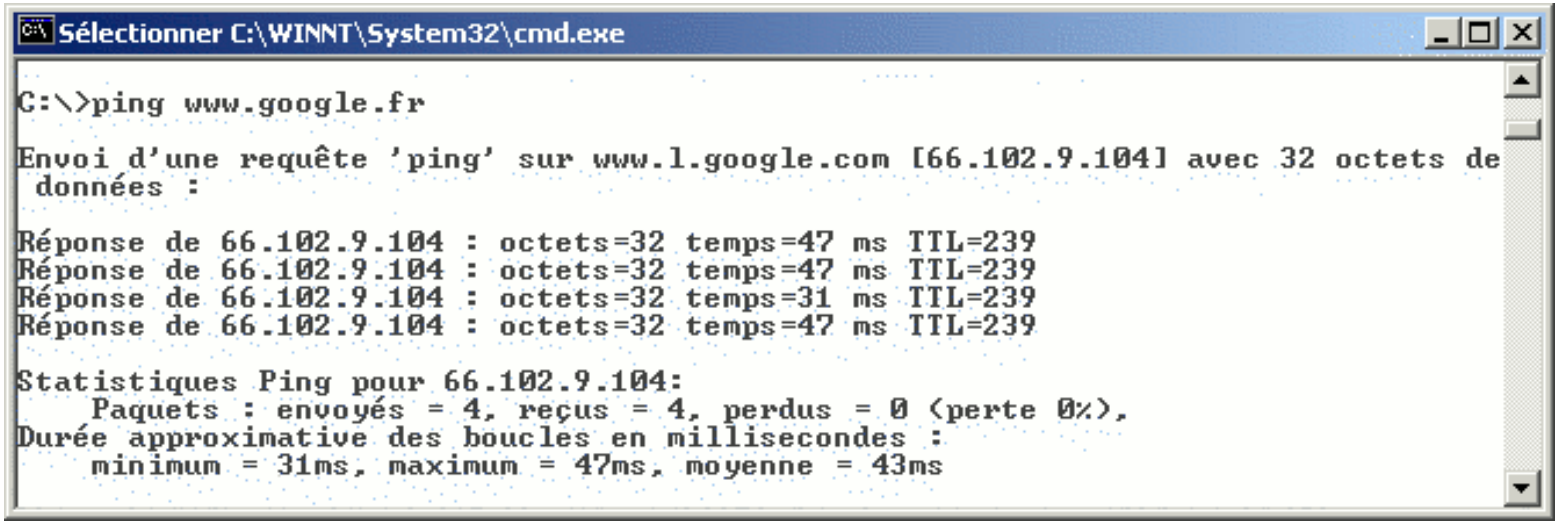
- La commande **ping** utilise les **paquets ICMP** de demande d'écho et de réponse en écho afin de déterminer si un système IP donné d'un réseau fonctionne.

- L'utilitaire **ping** est utilisé pour **diagnostiquer** les défaillances au niveau d'un réseau IP ou des routeurs.

La commande PING (2)

- **Ping @IP**





- **Ping Nom**

Chapitre 6 : Le routage IP

- 6.1 Le routage direct ou indirect
- 6.2 Le routage statique ou dynamique

Le routage IP

- Le routage est une fonction essentielle qui consiste à choisir le chemin pour transmettre un **datagramme IP** à travers les divers réseaux.

- On appelle **routeur** un équipement relié à **au moins deux réseaux** (cet équipement pouvant être un ordinateur, au sens classique du terme, qui assure les fonctionnalités de routage).

- un routeur ré-émettra des datagrammes venus d'une de ses interfaces vers une autre.

Routage IP direct

- Le **routage direct** correspond au **transfert** d'un datagramme au sein d'un **même réseau.** La démarche suivante est suivie :
  - L'expéditeur vérifie que le destinataire final partage le **même réseau** que lui. On utilise pour cela le masque de sous réseau.
  - Si c'est le cas, le **routage direct** est suffisant.
  - L'émission se fera en **encapsulant le datagramme** dans une **trame Ethernet**.

Routage IP indirect

- Le **routage indirect** est mis en œuvre dans tous les autres cas, c'est-à-dire quand au moins un **routeur** sépare **l'expéditeur initial** et le **destinataire final**. La démarche suivante est suivie :
  - L'expéditeur doit déterminer vers quel routeur envoyer un datagramme IP en fonction de sa destination finale.
  - Ceci est rendu possible par l'utilisation d'une table de routage spécifique à chaque routeur et qui permet de déterminer le prochain routeur destinataire pour transmettre le paquet.

La table de routage

- L'essentiel du contenu d'une table de routage est constitué de quadruplets:
  - **Destination** : C'est l'adresse IP d'une machine ou d'un réseau de destination.
  - **Passerelle (gateway)** : C'est l'adresse IP du prochain routeur vers lequel envoyer le datagramme pour atteindre cette destination
  - **Masque :** C'est le masque associé au réseau de destination
  - **Interface :** Cela désigne l'interface physique par laquelle le datagramme doit réellement être expédié.

La table de routage

Destination	Passerelle	Masque	Interface
C'est l'adresse IP d'une machine ou d'un réseau destination	*C'est l'adresse IP du prochain routeur vers lequel le datagramme est envoyé*	*C'est le masque associé au réseau de destination*	*Désigne l'interface physique (carte réseau) par laquelle le datagramme doit réellement être expédié.*

Une table de routage peut contenir une route par défaut qui spécifie un routeur par défaut vers lequel sont envoyés tous les datagrammes pour lesquels il n'existe pas de route dans la table

Remarques

- Tous les routeurs mentionnés dans une **table de routage** doivent être **directement accessibles** à partir du routeur considéré.

- Aucune machine, ni routeur ne connaît le chemin complet de routage des paquets. Chaque routeur connaît seulement le prochain routeur à qui le datagramme doit être envoyé.

Démarche du routage

- Supposons qu'une machine A souhaite envoyer une information une machine B.
- A compare la partie réseau de son adresse avec la partie réseau de l'adresse de B.
  1. =>Si A et B font partie du même réseau (ou sous-réseau). A envoie son information directement à B (routage direct).
  2. => Si A et B ne font pas partie du même réseau. A cherche, dans sa table de routage, la passerelle pour transmettre le datagramme.
  3. => Si A n'a toujours rien trouvé dans sa table de routage, il envoie l'information à la passerelle par défaut (default gateway).

Exemple de routage direct et indirect

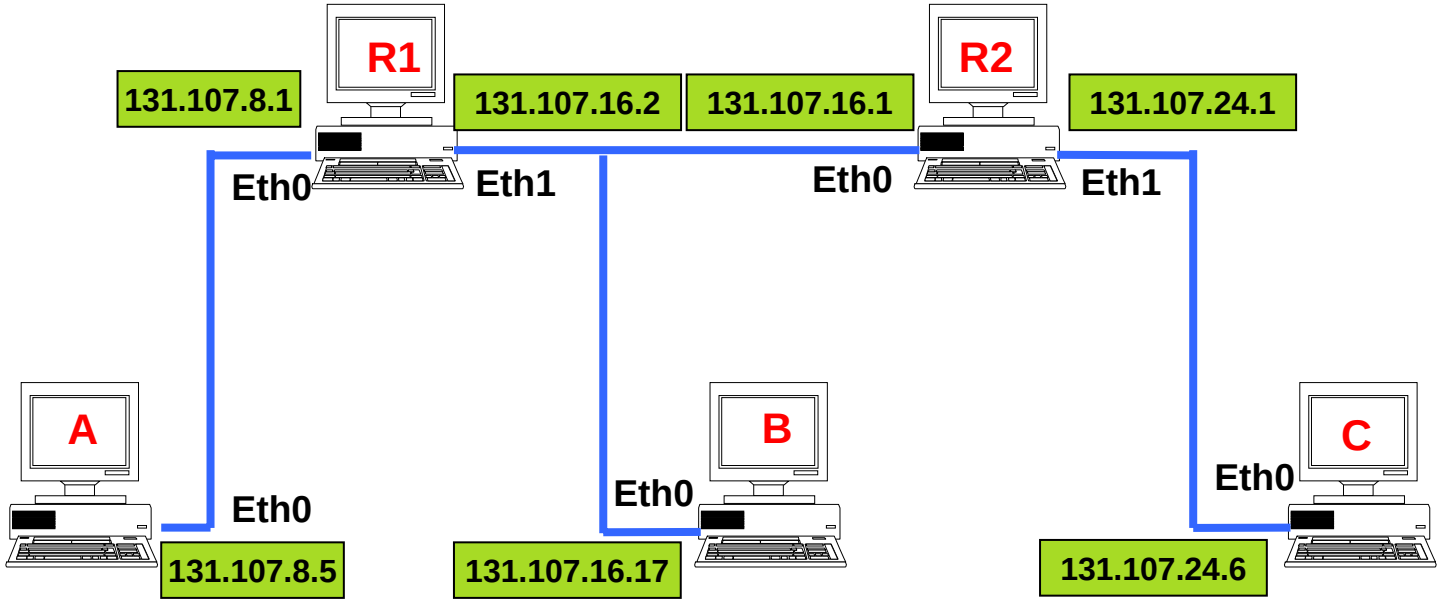
A (131.107.8.5) veut envoyer un paquet à C (131.107.24.6).

Table de routage de R1

Destination	Passerelle	Interface

Table de routage de R2

Destination	Passerelle	Interface

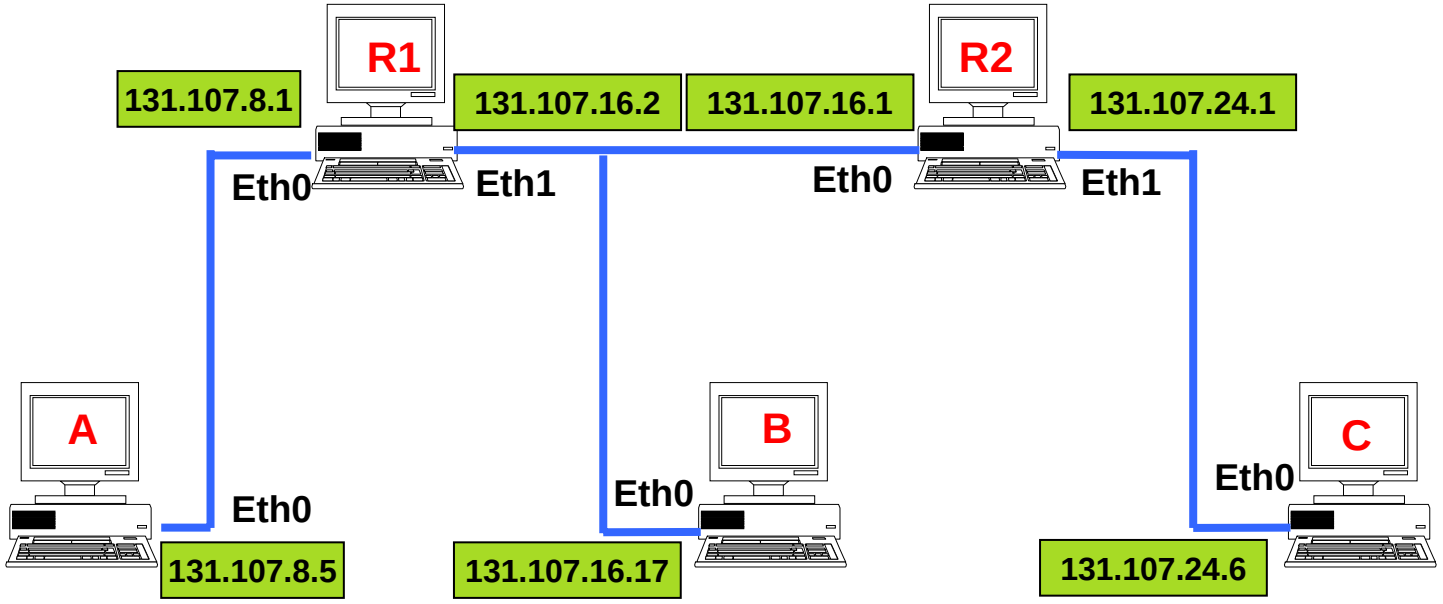


Exemple de routage direct et indirect

A (131.107.8.5) veut envoyer un paquet à C (131.107.24.6).

Table de routage de R1		
Destination	Passerelle	Interface
131.107.8.0 / 24	x	Eth0
131.107.16.0 / 24	x	Eth1
131.107.24.0 / 24	131.107.16.1	Eth1

Table de routage de R2		
Destination	Passerelle	Interface
131.107.16.0 / 24	x	Eth0
131.107.24.0 / 24	x	Eth1
131.107.8.0 / 24	131.107.16.2	Eth0



Chapitre 6 : Le routage IP

- 6.1 Le routage direct ou indirect
- 6.2 Le routage statique ou dynamique

Routage statique

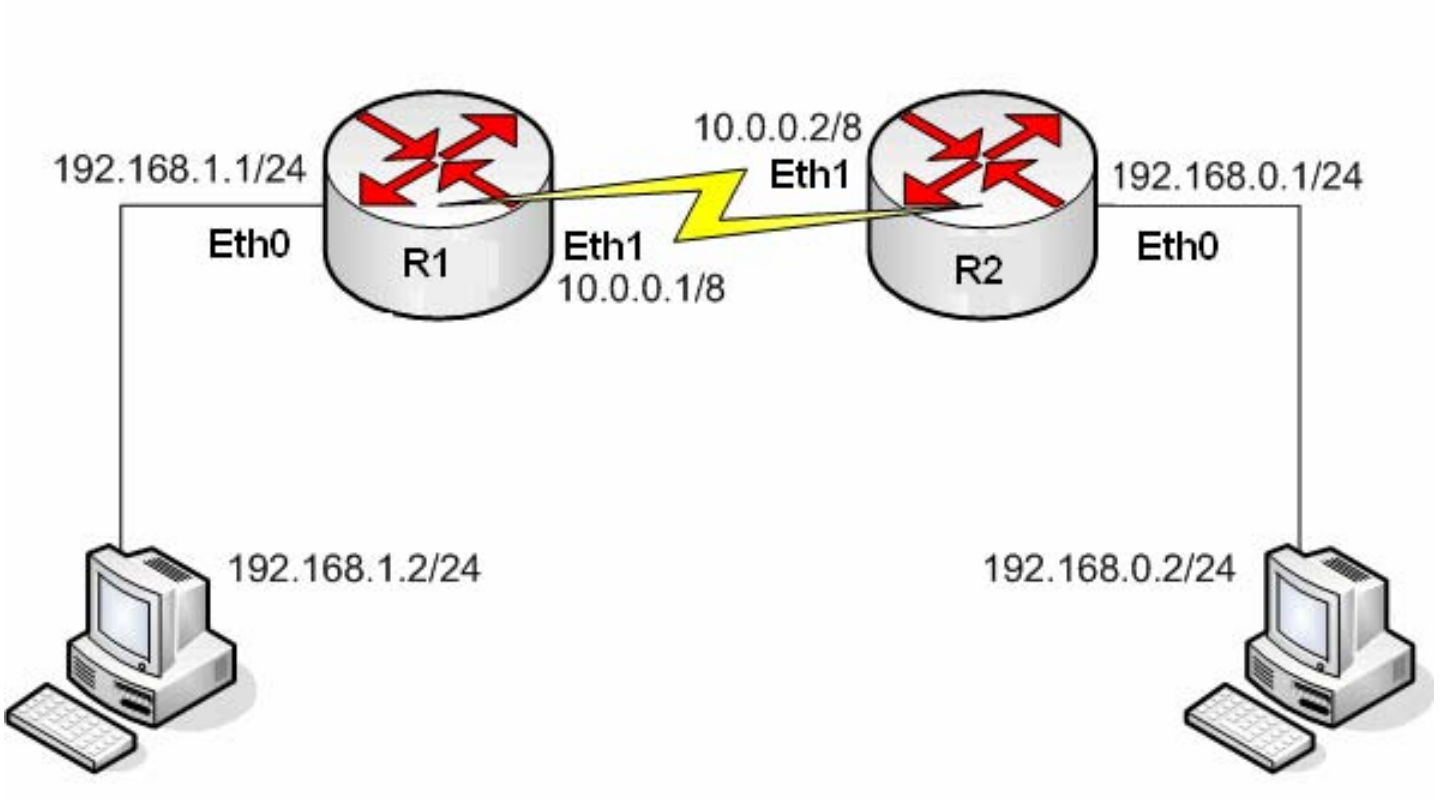
- **La table de routage est entrée manuellement** par l'administrateur et le routeur statique **ne partage pas** d'information avec les autres routeurs.

- Plus un réseau est important, plus cette tâche devient fastidieuse.

- Lorsque un nouveau réseau est ajouté, il faut reconfigurer l'ensemble manuellement. De plus, pour prévenir tout dysfonctionnement (panne d'un routeur, ligne coupée, etc.), il faut effectuer une surveillance permanente et **reconfigurer chaque routeur** le cas échéant.

Routage dynamique

Le routeur construit lui-même sa table de routage en fonction des informations qu'il reçoit des protocoles de routage. Il sélectionne la route la mieux adaptée à un paquet circulant sur le réseau en utilisant les informations d'état du réseau transmises d'un routeur à l'autre.



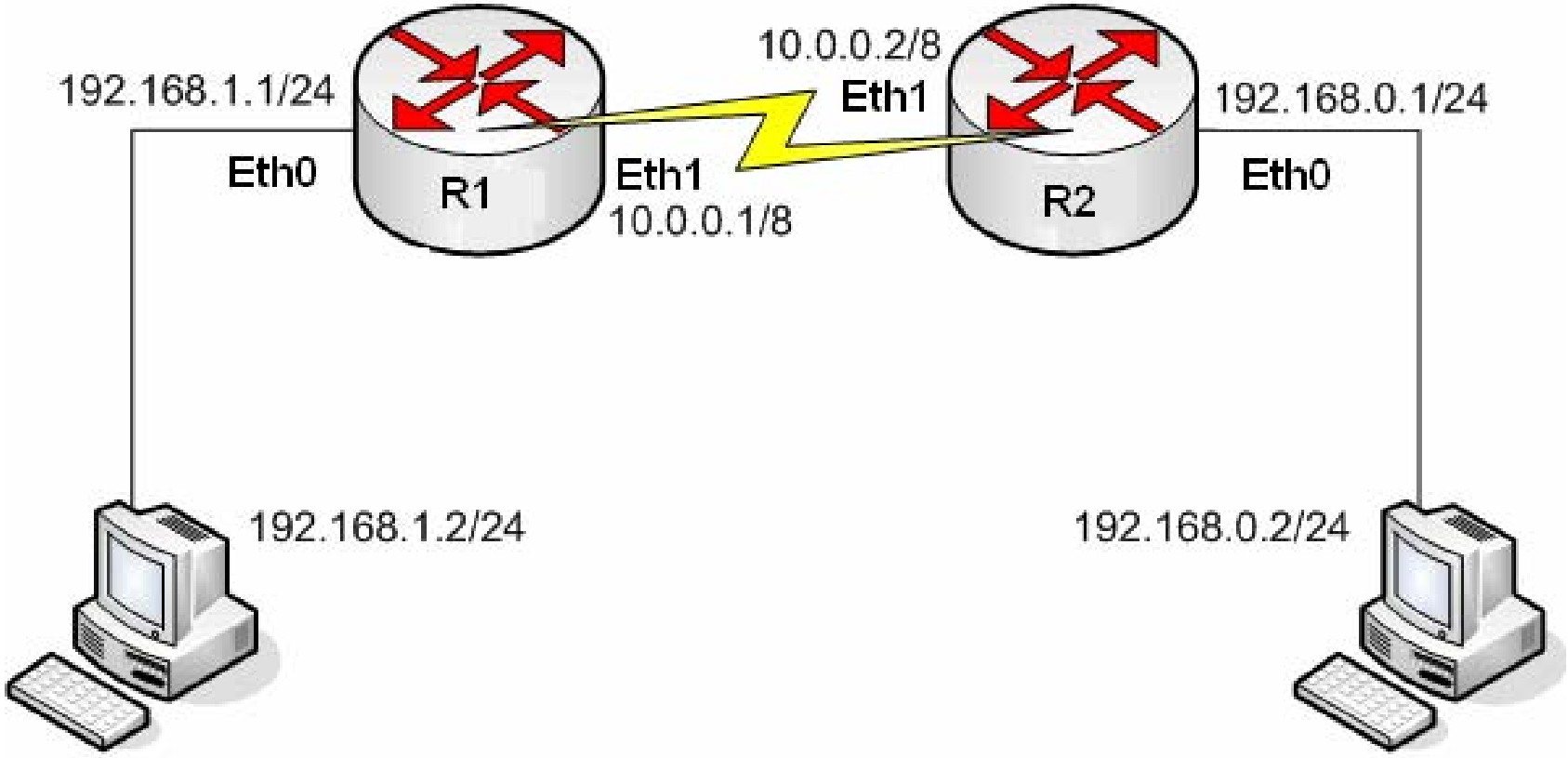
Le routage dynamique RIP

- Avec RIP,un routeur transmet à ses voisins les adresses réseaux qu'il connaît ainsi que la distance pour les atteindre.
  - Ces couples **adresse/distance** sont appelés **vecteurs de distance.**
- La métrique utilisée par RIP est la distance correspondant au nombre de routeurs à traverser (hop ou nombre de sauts) avant d'atteindre un réseau.
- Si plusieurs routes mènent à la même destination, le routeur doit alors choisir **la meilleure route** vers une destination donnée.
- Sur chaque routeur, si des routes redondantes apparaissent, il retient celle qui traverse **le moins de routeur.**

Le routage RIP : exemple (1)

- Exemple:

  Au départ aucune route n'est définie, puis on active le protocole RIP.



Le routage RIP : exemple (2)

- R1 et R2 construisent leur table en observant leurs interfaces :

Table de routage de R1			
Destination	Passerelle	Interface	Distance
100.0.0.0/8	**x**	**Eth1**	**1**
192.168.1.0/24	**x**	**Eth0**	**1**

Table de routage de R2			
Destination	Passerelle	Interface	Distance
100.0.0.0/8	**x**	**Eth1**	**1**
192.168.0.0/24	**x**	**Eth0**	**1**

- R1 transmet à R2 le vecteur de distance (192.168.1.0/24;1) et R2 transmet à R1 le vecteur de distance (192.168.0.0/24;1)
- Aucune information n'est transmise concernant le réseau 10.0.0.0/8, supposé connu par les deux routeurs.

Le routage RIP : exemple (3)

- R1 et R2 actualisent leurs tables avec les informations reçues:

Table de routage de R1			
Destination	Passerelle	Interface	Distance
100.0.0.0/8	**x**	**Eth1**	**1**
192.168.1.0/24	**x**	**Eth0**	**1**
192.168.0.0/24	**10.0.0.2**	**Eth1**	**2**

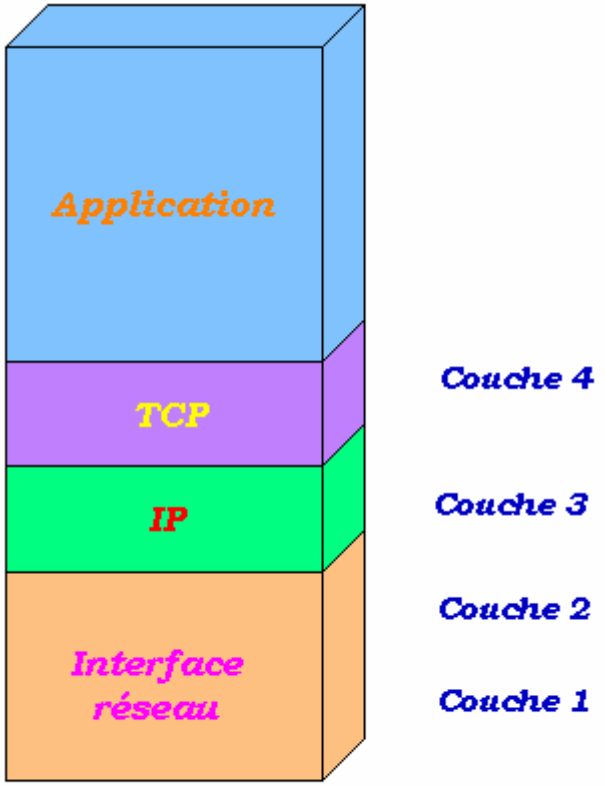
Table de routage de R2			
Destination	Passerelle	Interface	Distance
100.0.0.0/8	**x**	**Eth1**	**1**
192.168.0.0/24	**x**	**Eth0**	**1**
192.168.1.0	**10.0.0.1**	**Eth1**	**2**

Chapitre 7 : Les protocoles de couche 4 (TCP, UDP…)

- 7.1 Présentation du protocole TCP
- 7.2 Le segment TCP
- 7.3 Présentation du protocole UDP
- 7.4 La trame UDP
- 7.5 la translation d'adresse

Un protocole de couche 4 : TCP

- Grâce au protocole TCP, les applications peuvent communiquer de façon sûre (système d'accusés de réception), indépendamment des couches inférieures. Cela signifie que les routeurs (qui travaillent dans la couche Internet) ont pour seul rôle l'acheminement des données sous forme de datagrammes, sans se préoccuper du contrôle des données. Celui-ci est réalisé par la couche transport (Le protocole TCP).



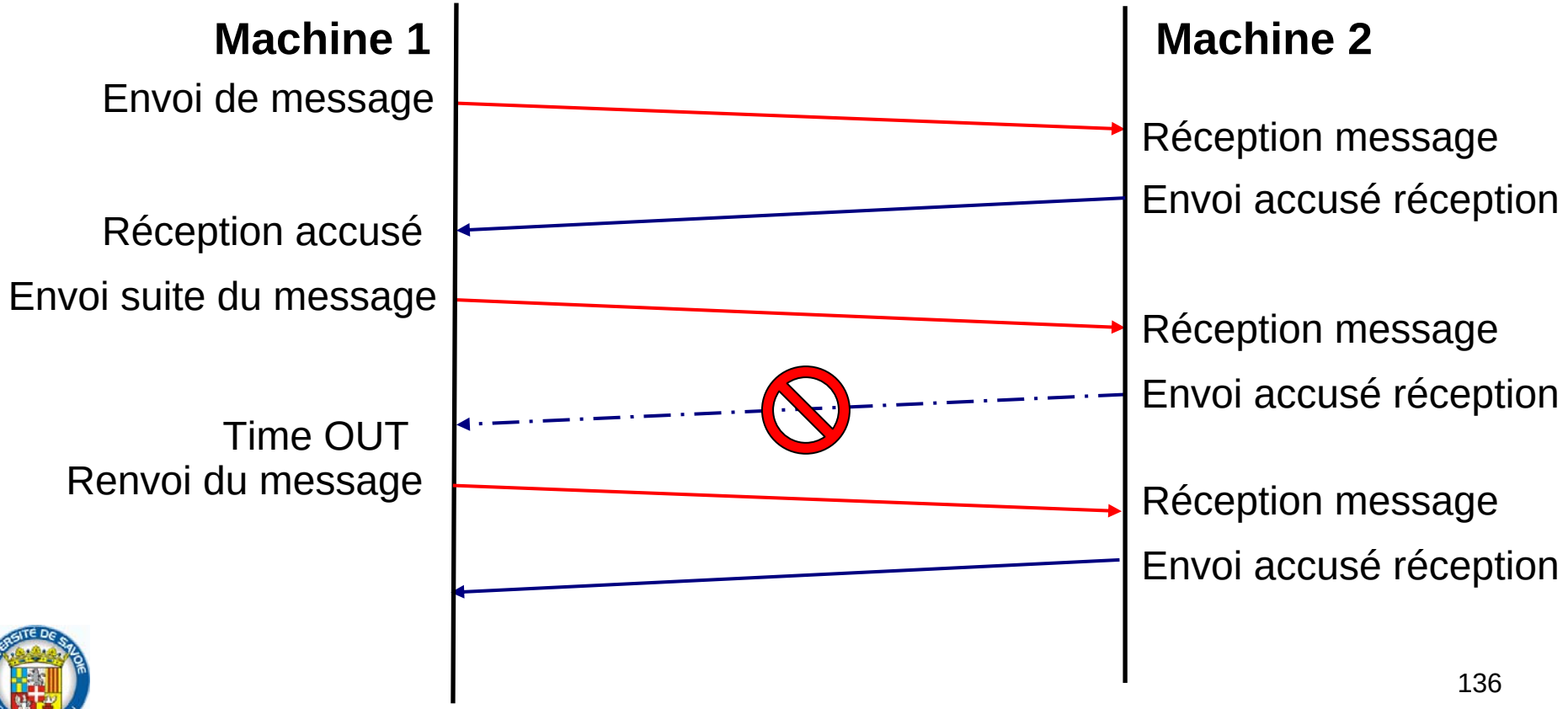
Standard TCP/IP

TCP (Transport Control Protocol)

- TCP (protocole IP numéro 6) est un protocole de transport :
  - **Orienté connexion :** il y a une connexion au début et une déconnexion à la fin du transfert du segment TCP.
  - **Fiable :** TCP fourni fournit un flux d'octet fiable assurant l'arrivée des données sans altération et dans l'ordre, avec retransmission en cas de perte, et élimination des données dupliquées.
  - **Faible rendement :** Le control du transfert de donnée augmente la quantité de donnée non utile.

Les acquittements

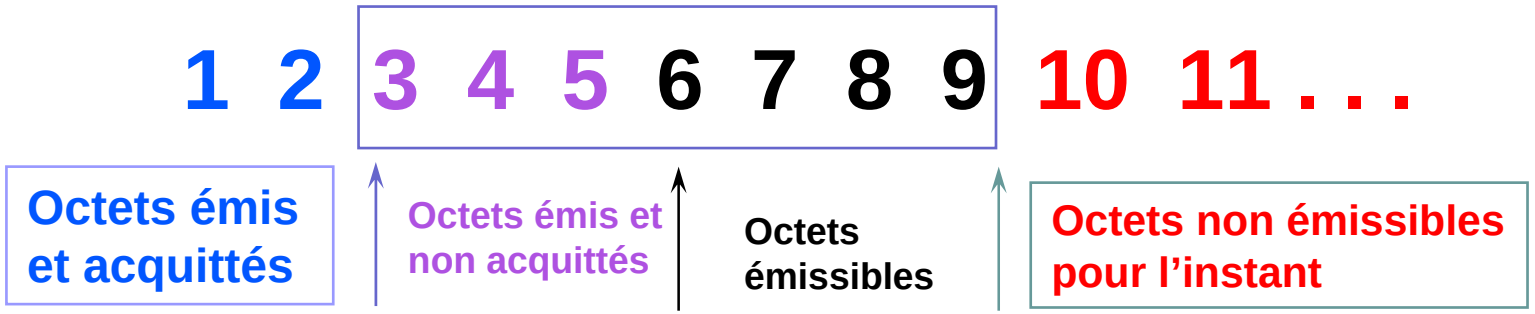
- Les acquittements sont des accusés de réception qui permettent de savoir si un message est bien arrivé à destination.



Le fenêtrage (1)

- Cette façon de procédé provoque un gaspillage de la bande passante !
  - Envoi de données
  - Attente
  - Envoi d’acquittement
  - Attente
  - …
- On peut optimiser grâce au fenêtrage

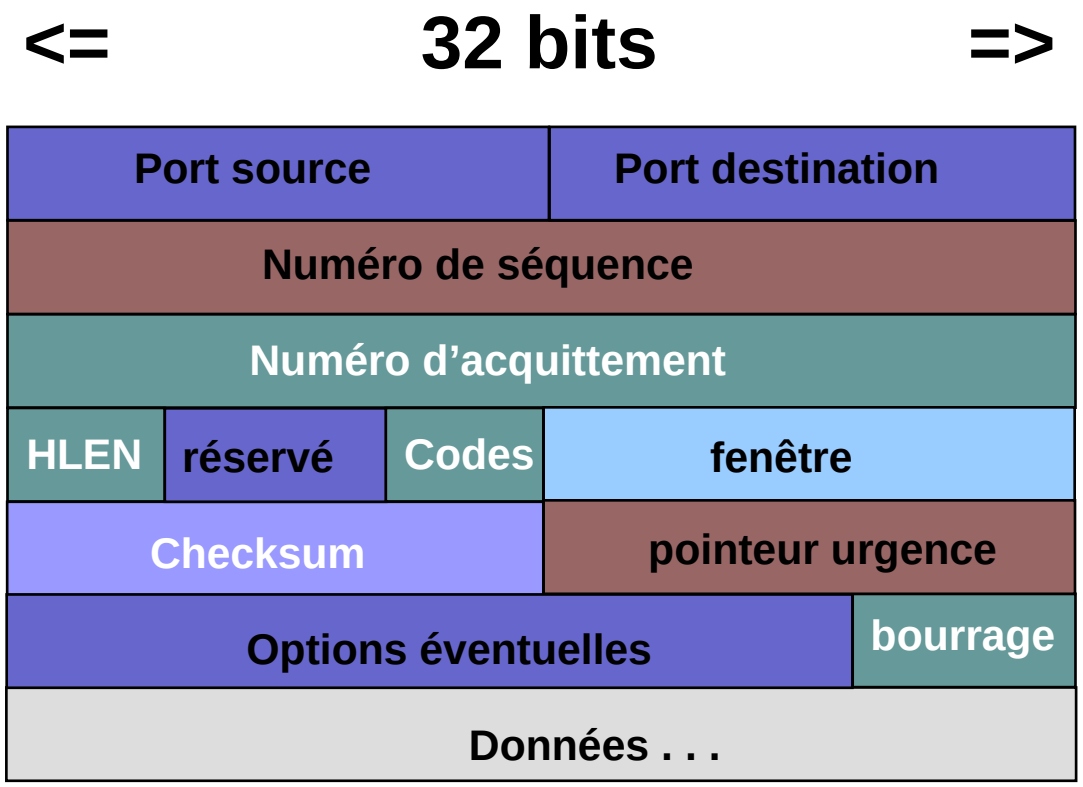
Le fenêtrage (2)



Chapitre 7 : Les protocoles de couche 4 (TCP, UDP…)

- 7.1 Présentation du protocole TCP
- 7.2 Le segment TCP
- 7.3 Présentation du protocole UDP
- 7.4 La trame UDP
- 7.5 La translation d'adresse

La trame TCP



Champ importants :

- Port source
- Port destination
- Numéro de séquence
- Numéro d'acquittement

Le protocole TCP : les Ports

- Quelle que soit **l'application cliente** (ex: navigateur Web), elle doit contacter le programme correspondant côté **serveur**. L'adresse **IP ne suffit pas.** En effet, l'@ IP indique seulement la machine serveur et non pas le service ou le **programme** sollicité sur la machine distante.

- Exemple :

  Vous envoyer une requête sur une machine distante possédant :
  - Un serveur de transfert de fichier (ftp)
  - Un serveur web (http)
  - Un service mail (pop et smtp)

  Comment préciser à quelle service vous faites appel?

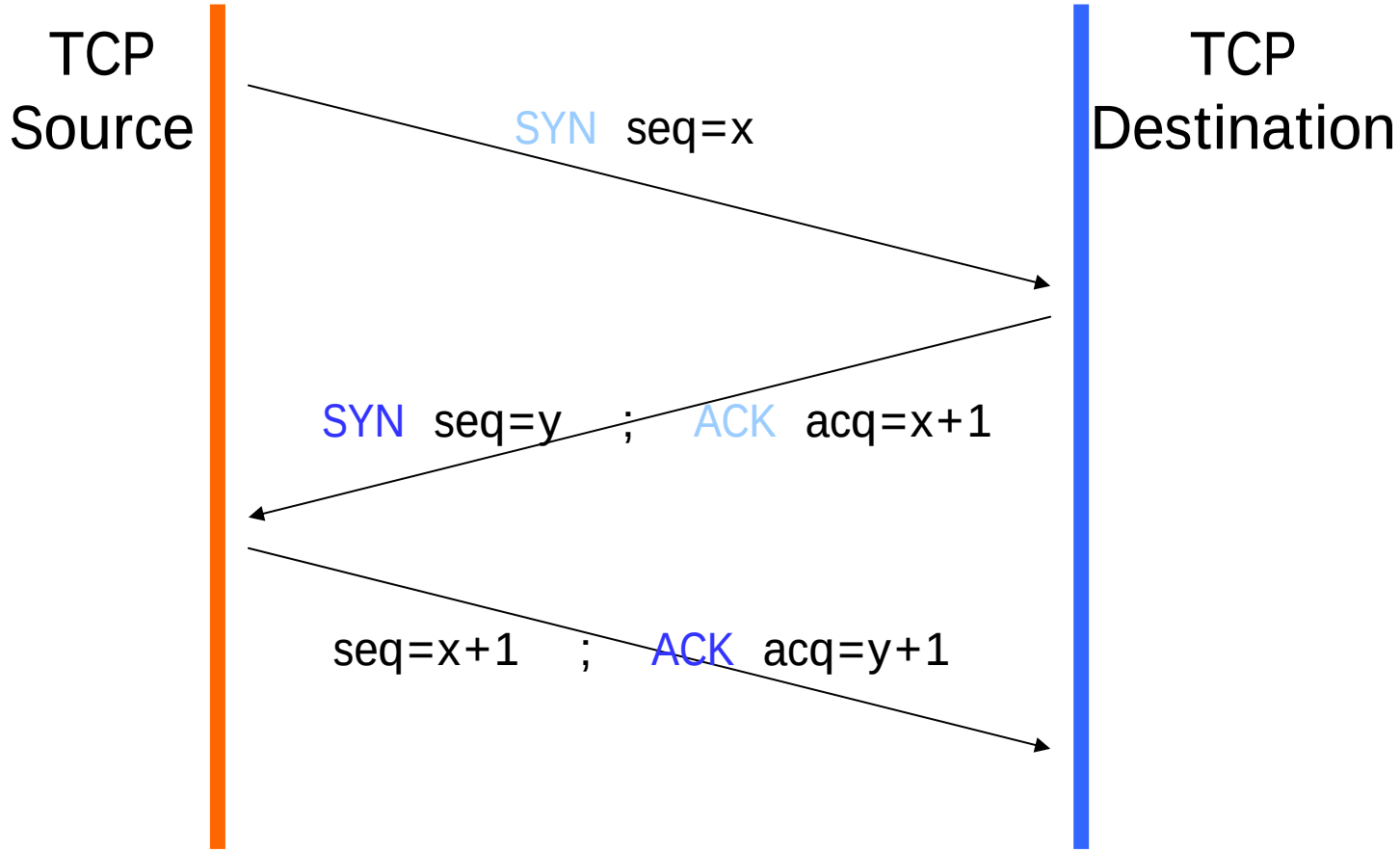
  REPONSE : En précisant un numéro de port

Le protocole TCP: les Ports

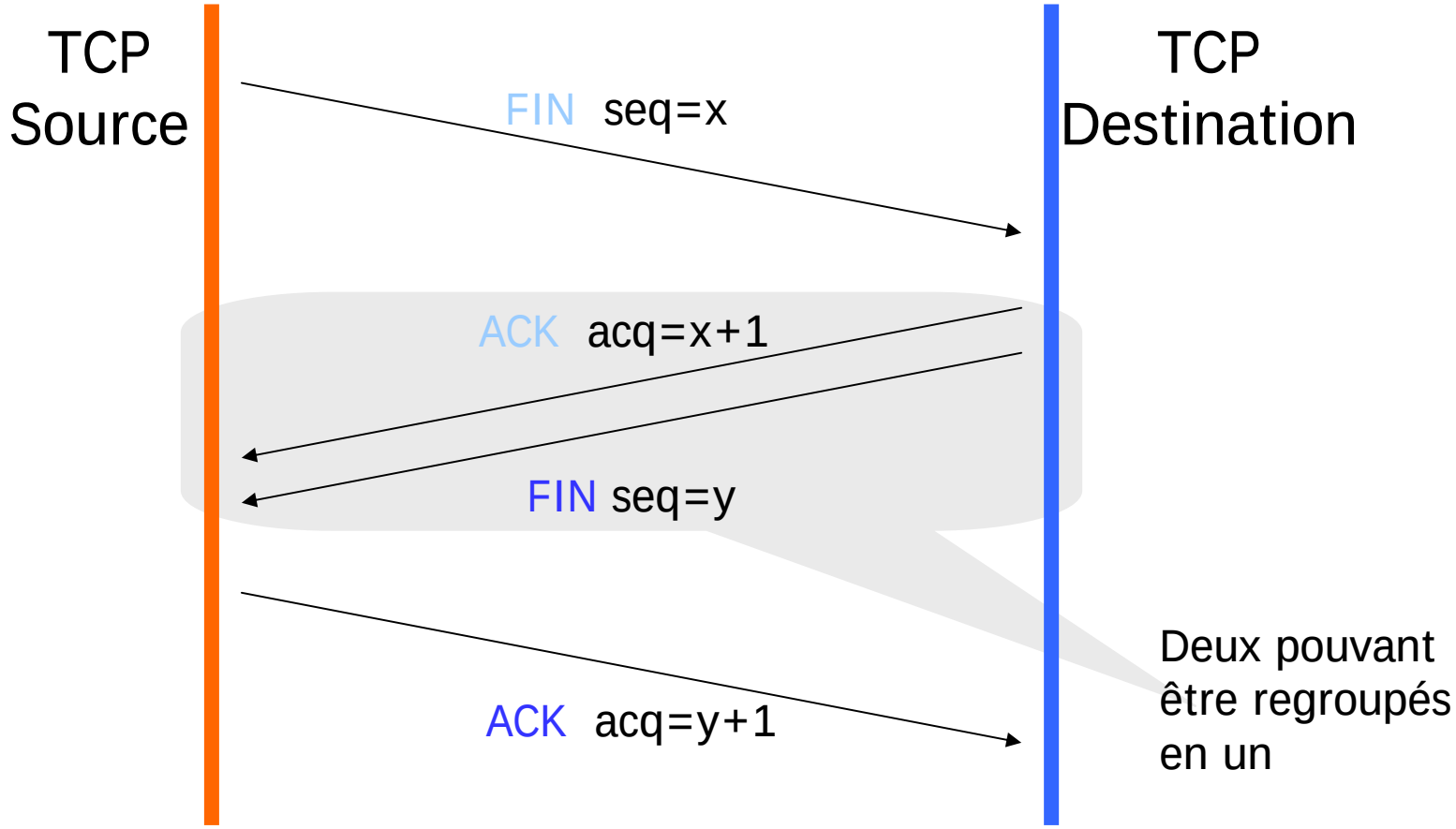
- Les applications courantes travaillent sur des ports bien définis suivantes (liste non exhaustive) :

Application / Service	***Port usuel***
HTTP	80
FTP	21
POP3	110
SMTP	25
NNTP (News)	119
Telnet	23
DNS	53

Le protocole TCP: connexion



Le protocole TCP: déconnexion



Conclusion

- La couche 4 améliore les services de couche 3
  - UDP
    - Protocole très léger
  - TCP
    - Full-Duplex
    - Service garanti
      - Acknowledges ➔ arrivée garantie des segments
      - Séquençage ➔ ordre garanti des segments
      - Acknowledges cumulés ➔ pas *trop* de gaspillage

Chapitre 7 : Les protocoles de couche 4 (TCP, UDP…)

- 7.1 Présentation du protocole TCP
- 7.2 La segment TCP
- 7.3 Présentation du protocole UDP
- 7.4 La trame UDP
- 7.5 la translation d'adresse

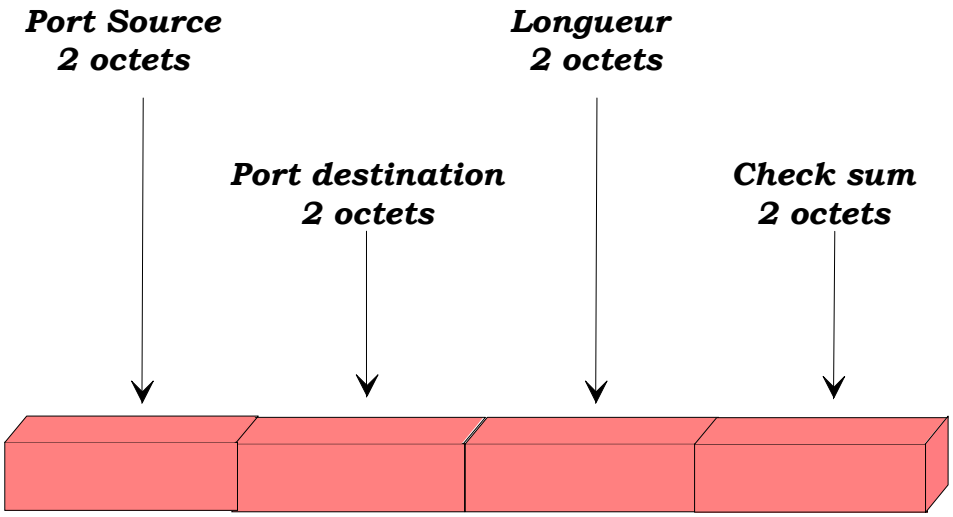
Protocole de couche 4 : UDP

- Le protocole UDP (User Datagram Protocol) est un protocole non orienté connexion de la couche transport du modèle TCP/IP. Ce protocole est très simple étant donné qu'il ne fournit pas de contrôle d'erreurs (il n'est pas orienté connexion...).

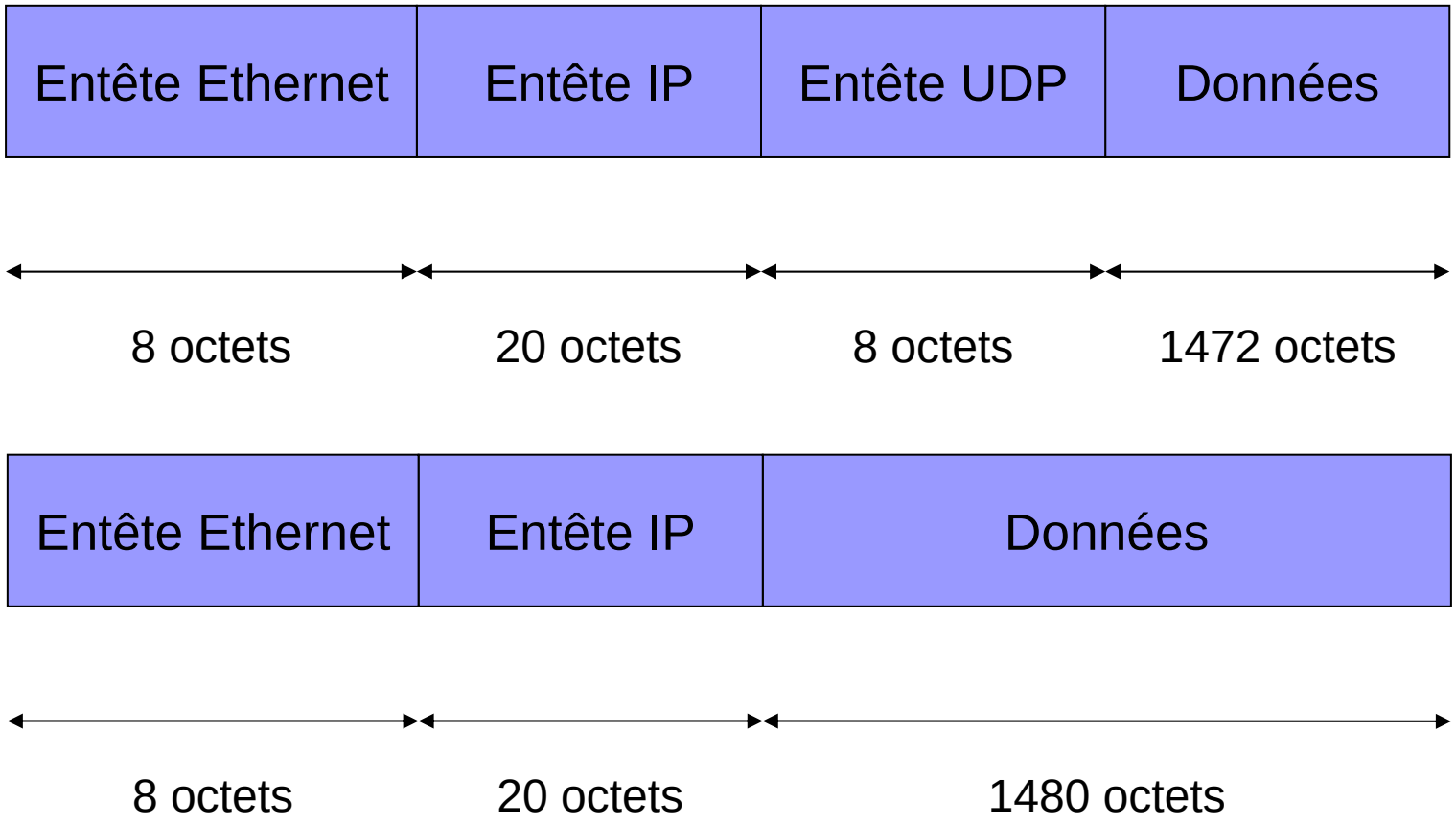
Chapitre 7 : Les protocoles de couche 4 (TCP, UDP…)

- 7.1 Présentation du protocole TCP
- 7.2 La segment TCP
- 7.3 Présentation du protocole UDP
- 7.4 La trame UDP
- 7.5 la translation d'adresse

Trame UDP


Port Source
2 octets
Port destination
2 octets
Longueur
2 octets
Check sum
2 octets

Trame UDP encapsulée



Chapitre 7 : Les protocoles de couche 4 (TCP, UDP…)

- 7.1 Présentation du protocole TCP
- 7.2 Le segment TCP
- 7.3 Présentation du protocole UDP
- 7.4 La trame UDP
- 7.5 la translation d'adresse

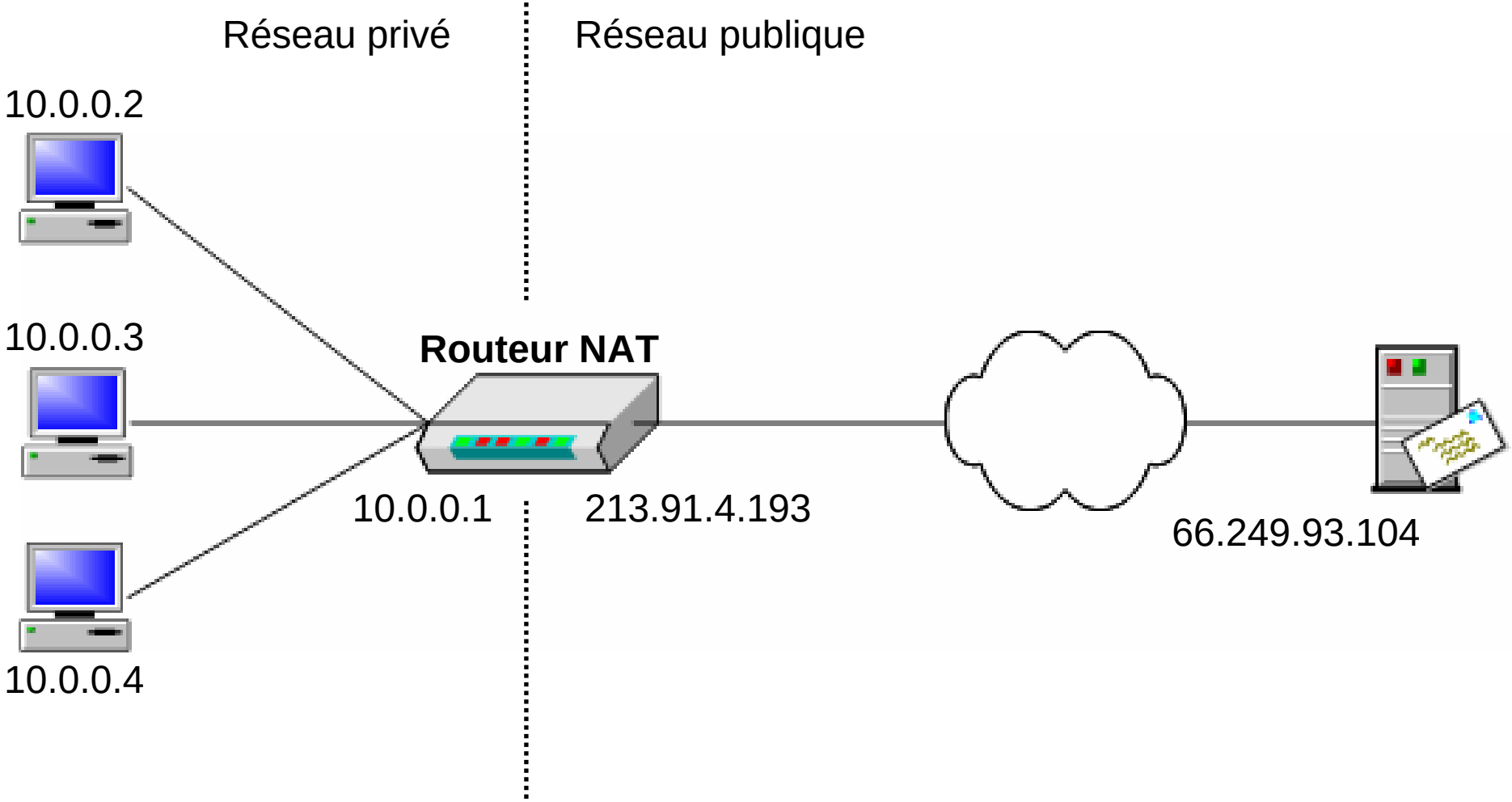
La translation d’adresse

- Pourquoi le NAT ?

  Le mécanisme de translation d'adresses (en anglais Network Address Translation noté NAT) a été mis au point afin de répondre à la pénurie d'adresses IP avec le protocole IPv4 (le protocole IPv6 répondra à terme à ce problème).

- Le principe du NAT consiste donc à utiliser une passerelle de connexion à internet, possédant au moins une interface réseau connectée sur le réseau privé et au moins une interface réseau connectée à Internet (possédant une adresse IP routable).

La translation d’adresses

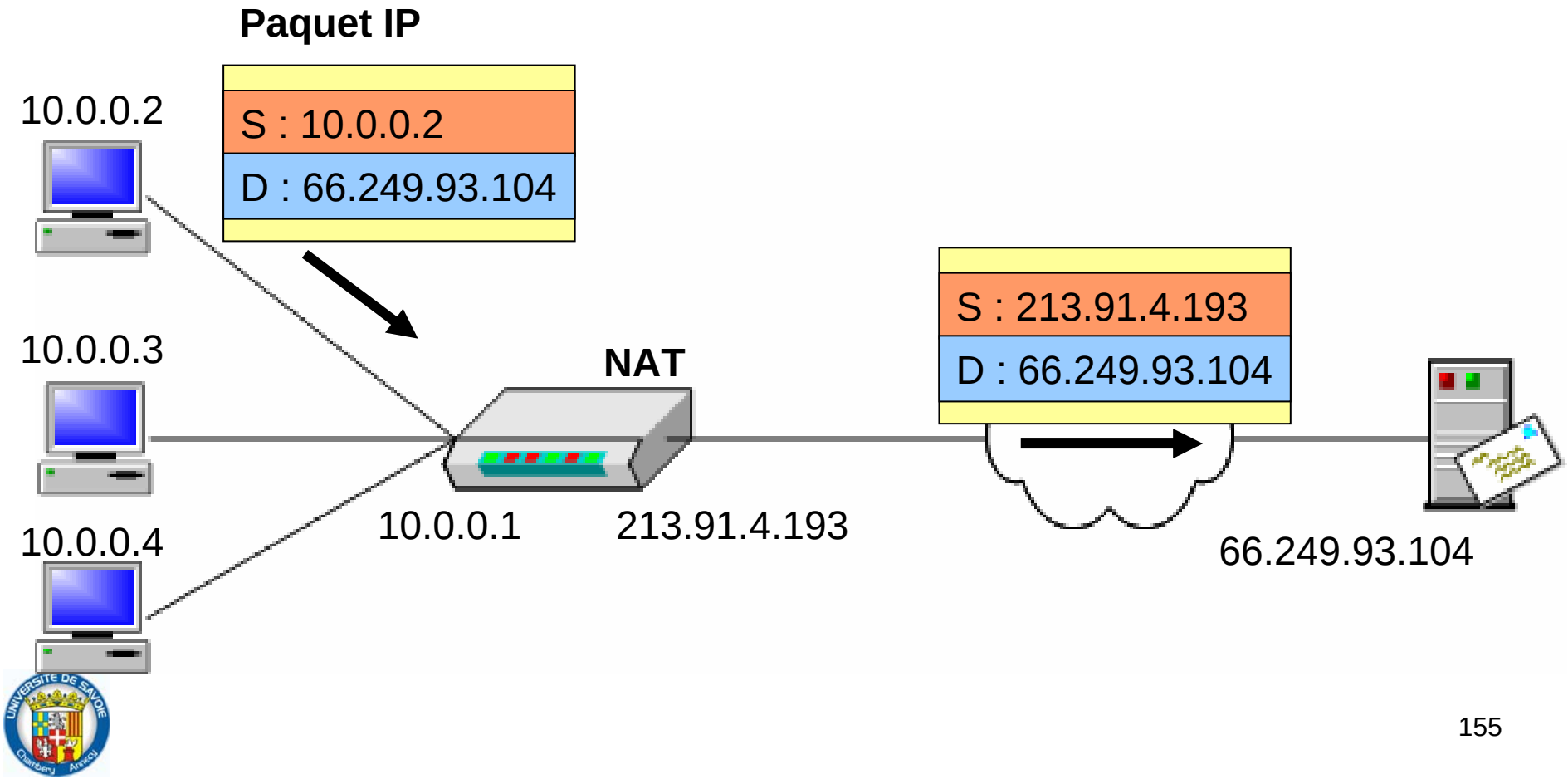


La translation d'adresses (NAT)

- Si une seule adresse IP publique est partagée entre plusieurs stations, la passerelle doit effectuer une translation d'adresses pour les paquets entrant et sortant
  - L'adresse IP source des paquets sortant est remplacée par l'adresse publique
  - L'adresse IP de destination des paquets entrant est remplacée par l'adresse privée de la station cible

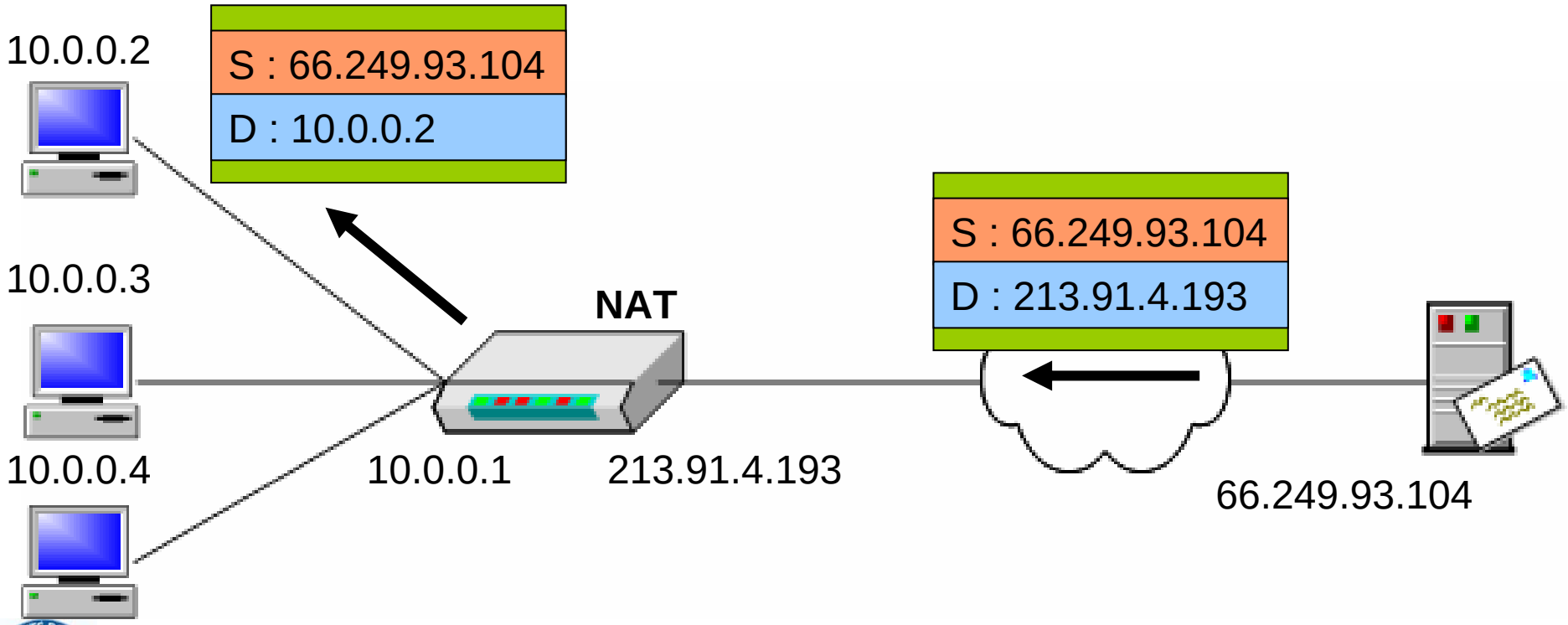
NAT des paquets sortants (1)

- Lorsqu'une machine du réseau effectue une requête vers Internet, la passerelle effectue la requête à sa place.



NAT des paquets rentrants (1)

- Près réception, la réponse est transmise à la machine ayant fait la demande.

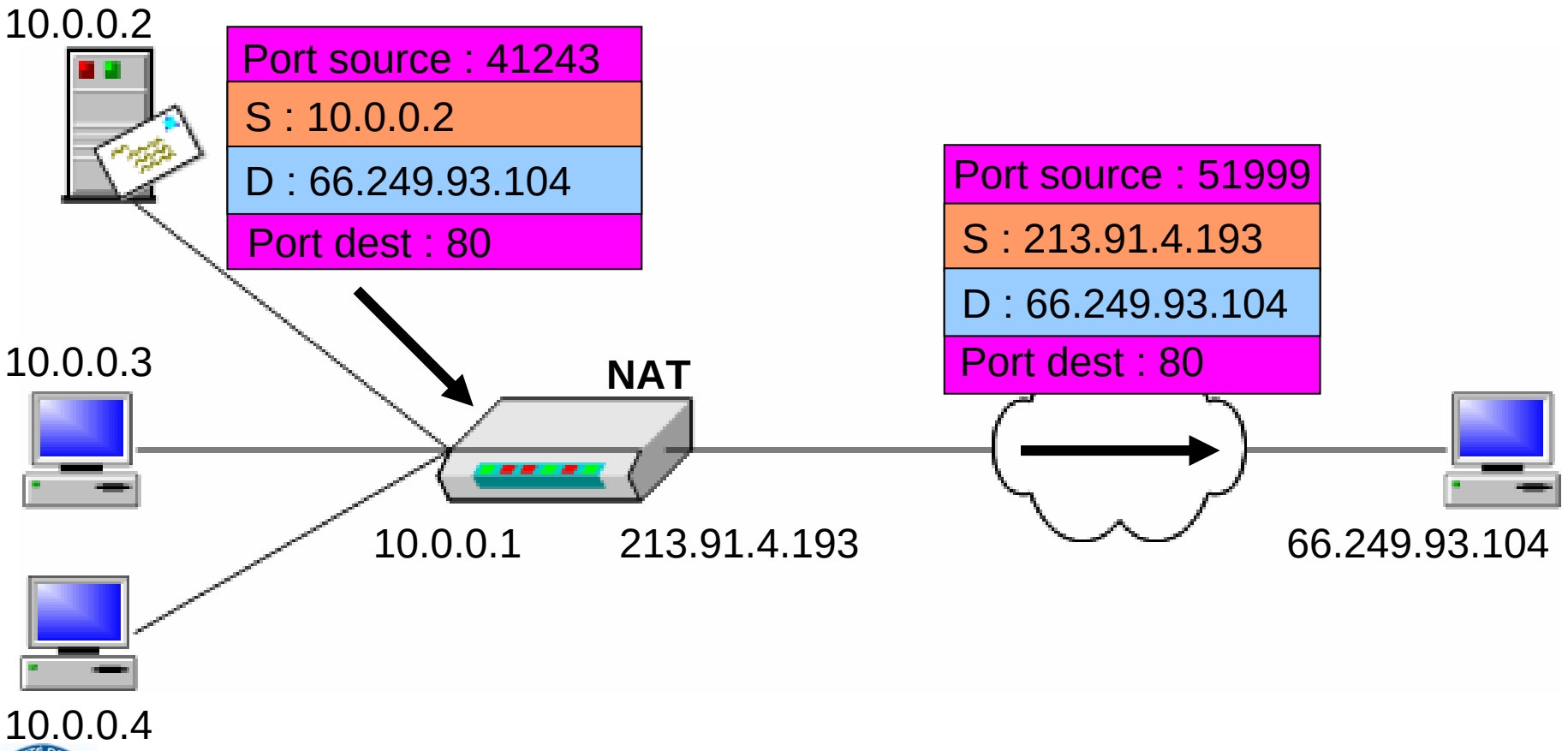


La translation d’adresses (NAT)

- Problème :
  - Si deux machines du réseau interne effectue deux requete simultanée, comment fait t on pour savoir à qui correspond les réponses des requêtes que le routeur va recevoir?

- Solution :
  - Le NAT dynamique utilise le mécanisme de translation de port (PAT - Port Address Translation), c'est-à-dire l'affectation d'un port source différent à chaque requête.

NAT des paquets sortants (2)



NAT des paquets rentrants (2)

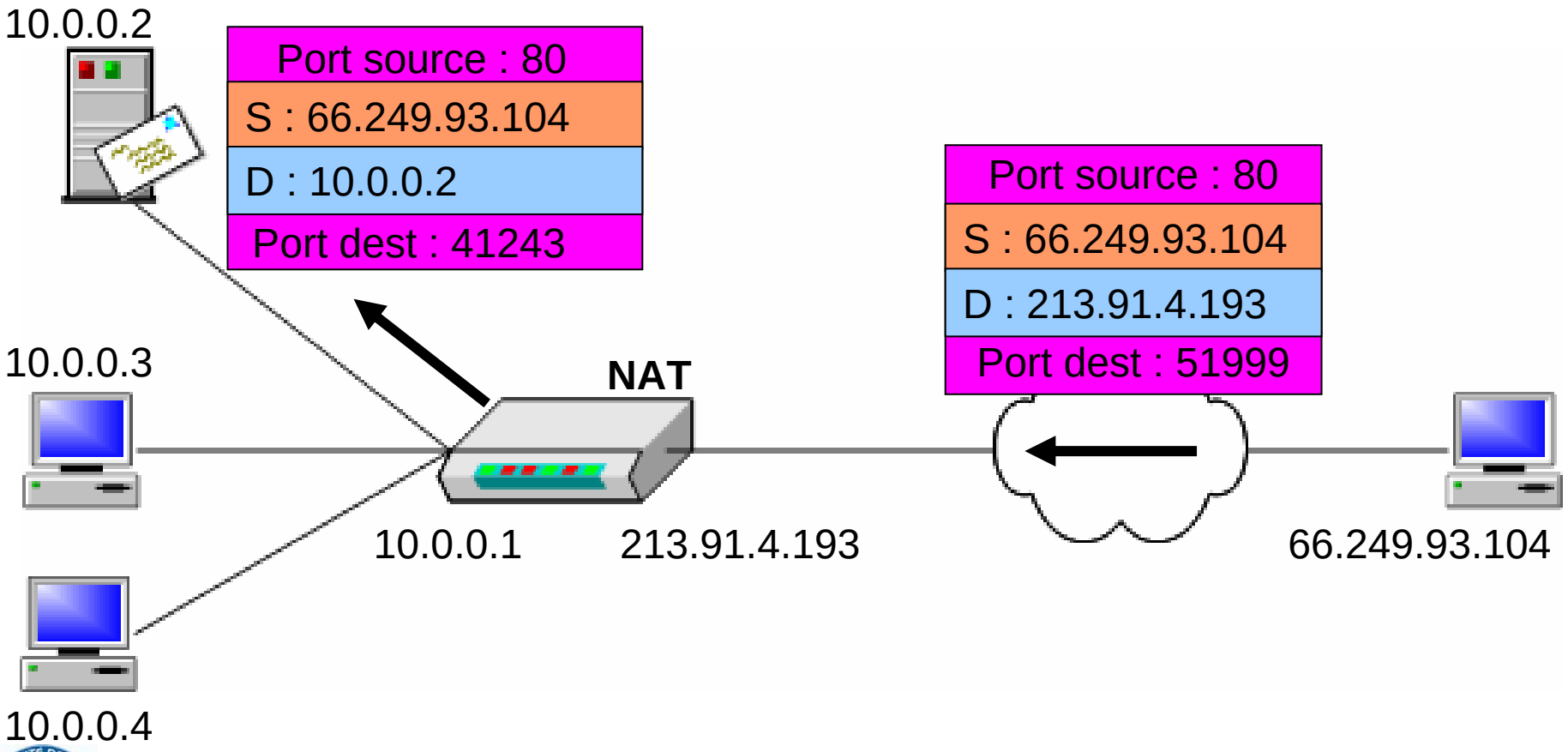


Table des translations

- Le routeur NAT va conserver une table des translations lui permettant de conserver la tracer de l'émetteur.

Interne		**Externe**
@IP	Ports	Ports
10.0.0.1	1035	1035
10.0.0.2	41243	51999
10.0.0.3	1035	1033
10.0.0.4	1025	1025

NAT & sécurité

- Remarques sur le NAT :

  Étant donné que la passerelle camoufle complètement l'adressage interne d'un réseau, le mécanisme de translation d'adresses permet d'assurer une fonction de sécurisation. En effet, pour un observateur externe au réseau, toutes les requêtes semblent provenir de l'adresse IP de la passerelle.

Chapitre 8 : Les protocoles applicatifs (HTTP, SMTP, DNS...)

- 8.1 Présentation du protocole DHCP
- 8.2 Présentation du protocole HTTP
- 8.3 Présentation du protocole DNS

Le Protocole DHCP

- Dans un réseau, chaque station doit avoir ses propriétés TCP/IP configurées correctement. Il faut renseigner :
  - L'adresse IP,
  - Le masque réseau,
  - La passerelle par défaut,
  - L'adresse du serveur DNS, etc…
- Si l'administrateur du réseau doit effectuer ce paramétrage sur un grand nombre d'ordinateurs, cela peut induire des erreurs (ex: double utilisation d'une même adresse IP), et faire perdre du temps.
- Une solution: le protocole DHCP (Dynamic Host Configuration Protocol) permet de rendre automatique ces configurations.

Le Protocole DHCP

- Lors du démarrage, les stations utilisant DHCP envoient une requête (Broadcast). Lorsque le serveur DHCP reçoit cette requête, il choisit les paramètres TCP/IP pour le client et les lui transmet (Broadcast).

- Un serveur DHCP délivre donc automatiquement des adresses IP aux stations qui se connectent, il faut alors indiquer la plage d'adresses que le serveur DNS est autorisé à distribuer.

Le Protocole DHCP : remarques

- Les adresses IP distribuées ont une date de début et une date de fin de validité. C'est ce qu'on appelle un « bail ».
- On peut optimiser l'attribution des adresses IP en jouant sur la durée des baux.
- Sur un réseau où beaucoup d'ordinateurs se connectent et se déconnectent souvent (réseau d'école ou de locaux commerciaux par exemple), des baux de courte durée sont intéressants.
- Sur un réseau constitué en majorité de machines fixes, très peu souvent rebootées, des baux de longues durées suffisent.
- DHCP fonctionne principalement par broadcast, cela peut bloquer de la bande passante sur des petits réseaux fortement sollicités.

Chapitre 8 : Les protocoles applicatifs (http, SMTP, DNS…)

- 8.1 Présentation du protocole DHCP
- 8.2 Présentation du protocole HTTP
- 8.3 Présentation du protocole DNS

HTTP : Hyper Text Transfert Protocol

- Le but du protocole HTTP est de permettre un transfert de fichiers (essentiellement au format HTML) localisés grâce à une chaîne de caractères appelée URL entre un navigateur (le client) et un serveur Web. La communication se fait en deux temps :
  - Requête HTTP émise par le client.
  - Réponse HTTP envoyée par le serveur (après traitement de la requête)

URL (Uniform Resource Locator)

Une URL (Uniform Resource Locator) est un format de nommage universel pour désigner une ressource sur Internet. Il s'agit d'une chaîne de caractères ASCII imprimables qui se décompose en cinq parties :

- Le nom du protocole : C'est le langage utilisé pour communiquer sur le réseau. Le protocole le plus utilisé est http. De nombreux autres protocoles sont toutefois utilisables (FTP,News,Mailto,...)
- Identifiant et mot de passe : Permet de spécifier les paramètres d'accès à un serveur sécurisé. Cette option est déconseillée car le mot de passe est visible dans l'URL.
- Le nom du serveur : Il s'agit d'un nom de domaine de l'ordinateur hébergeant la ressource demandée. Notez qu'il est possible d'utiliser l'adresse IP du serveur, ce qui rend par contre l'URL moins lisible.
- Le numéro de port : il s'agit d'un numéro associé à un service permettant au serveur de savoir quel type de ressource est demandée. Le port associé par défaut au protocole est le port numéro 80.
- Le chemin d'accès à la ressource : Cette dernière partie permet au serveur de connaître l'emplacement auquel la ressource est située, c'est-à-dire de manière générale l'emplacement (répertoire) et le nom du fichier demandé

Exemple d'URL

Protocole	Mot de passe (facultatif)	Nom du serveur	Port	Chemin
http://	user:password@	www.univ-savoie.fr	:80	/glossair/glossair.php3

Chapitre 8 : Les protocoles applicatifs (http, SMTP, DNS…)

- 8.1 Présentation du protocole DHCP
- 8.2 Présentation du protocole HTTP
- 8.3 Présentation du protocole DNS

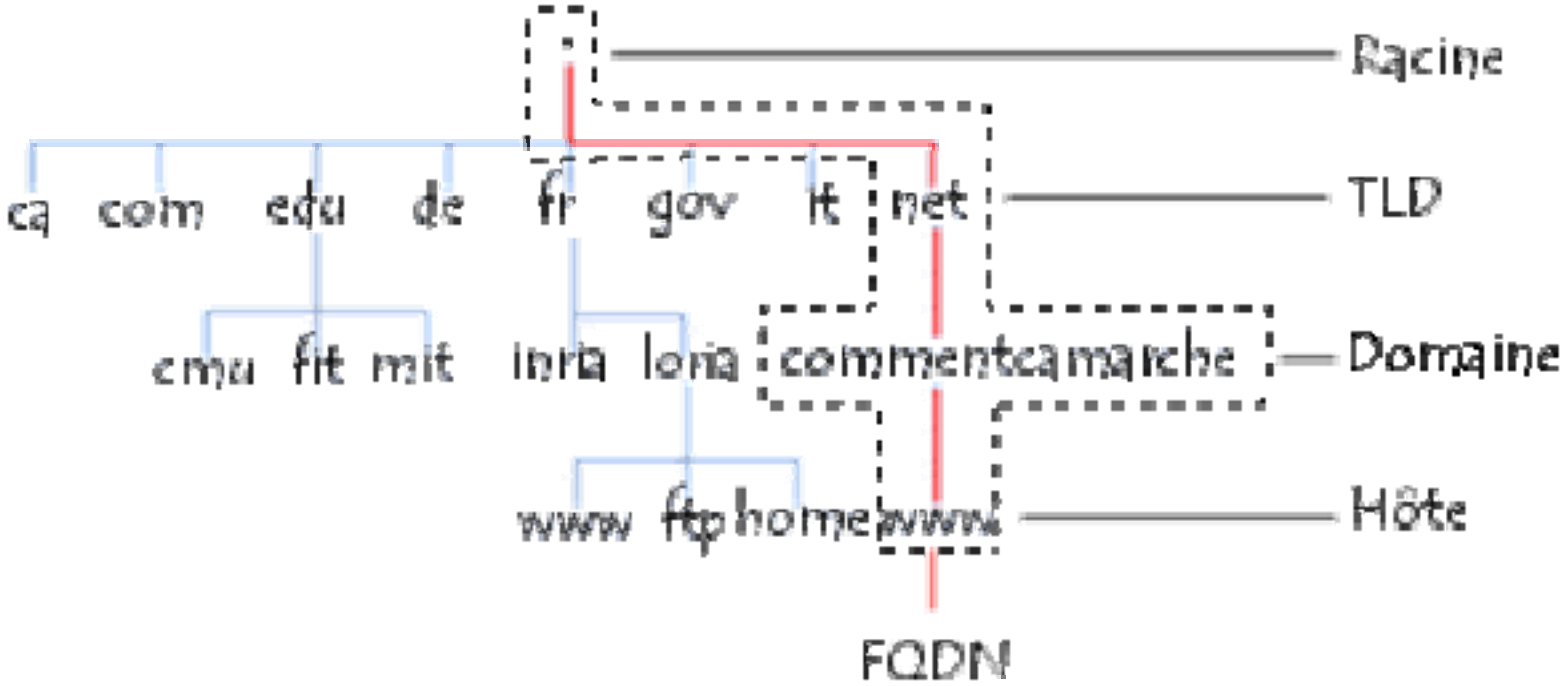
Le DNS : Domain Name System

- Un site est toujours localisé sur Internet par l'adresse IP de la machine sur laquelle il se trouve. Mais on indique généralement au navigateur le nom de domaine du site que l'on souhaite visiter, et non pas son adresse IP.

- Un navigateur web, pour se rendre sur un site, doit donc connaître l'adresse IP du nom de domaine correspondant. Il faut donc faire la correspondance entre un nom de domaine et son adresse IP.

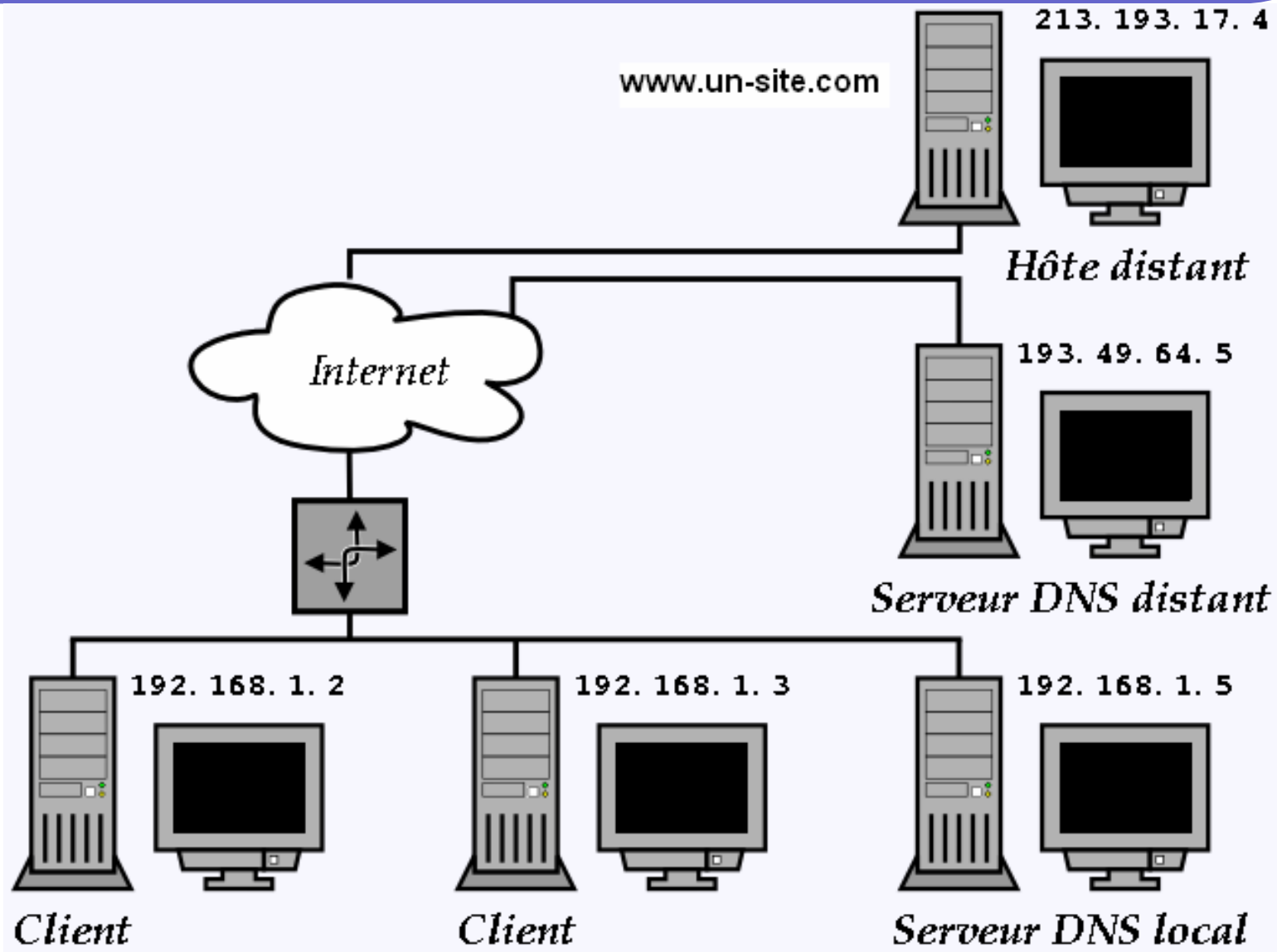
- Si les services de correspondance sont hors service, aucun navigateur ne pourra connaître l'adresse IP du site correspondant, et donc consulter ce site.

Le DNS : Domain Name System



TLD = Top Level Domains
FQDN = Fully Qualified Domain Name

Le DNS : Organisation



DNS: Serveurs de noms de domaines

Imaginons qu'une machine de l'université (192.168.1.2) cherche à communiquer avec le site http://www.un-site.com.

- La machine du réseau de l'université va envoyé une requête au serveur de noms défini dans sa configuration réseau (Serveur DNS local, 192.168.1.5). Chaque machine connectée au réseau possède en effet dans sa configuration les adresses IP de deux serveurs de noms de son fournisseur d'accès :
  - Serveur de nom primaire (appelé Serveur DNS local dans notre cas)
  - Serveur de nom secondaire (qui intervient si le premier tombe en panne)

- Si celui-ci possède l'enregistrement dans son cache, il l'envoie à l'application. Dans le cas contraire le DNS de l'université interroge un serveur racine (dans notre cas un serveur racine correspondant au TLD « .com »). Le serveur de nom racine renvoie une liste de serveurs de noms faisant autorité sur le domaine « un-site.com ».

- Le serveur de noms primaire faisant autorité sur le domaine « un-site.com » va alors être interrogé par le serveur DNS de l'université et retourner l'enregistrement correspondant à l'hôte sur le domaine (dans notre cas www).