Cours Réseaux - Généralités

La Salle Avignon

v0.1

Frères des Ecoles Chrétiennes
Saint-Jean-Baptiste de la Salle - Avignon

Sommaire

Frères des Ecoles Chrétiennes
Saint-Jean-Baptiste de la Salle - Avignon

Définition

Un réseau désigne un **ensemble d'équipements interconnectés pour permettre la communication de données entre applications, quelles que soient les distances qui les séparent**.
Un réseau s'appuie sur deux notions fondamentales :

- L'**interconnexion** qui assure la transmission des données d'un noeud à un autre.
- La **communication** qui permet l'échange des données entre processus.

On appelle noeud (*node*) l'extrémité d'une connexion. Un processus est un programme en cours d'exécution et représente le bout d'une communication dans un réseau informatique.

Frères des Ecoles Chrétiennes Saint-Jean-Baptiste de la Salle - Avignon

Caractéristiques

Les caractéristiques de base d'un réseau sont :

- La **topologie** qui définit l'architecture d'un réseau : on distinguera la **topologie physique** qui définit la manière dont les équipements sont interconnectés entre eux, de la **topologie logique** qui précise la manière dont les équipements communiquent entre eux.
- Le **débit** exprimé en bits/s (ou bps) qui mesure une quantité de données numériques (bits) transmises par seconde (s).
- La **distance maximale** (ou portée) qui dépend de la technologie mise en oeuvre.
- Le **nombre de noeuds** maximum que l'on peut interconnecter.

Éléments d'un réseau

Il faut un ensemble d'équipements **matériels** et **logiciels**.
On peut citer par exemple :

- une carte de communication, des supports "physiques" (câbles paires cuivre torsadées, fibre optique, prises RJ45, WIFI, CPL, ligne téléphonique, ADSL, ...) et des équipements d'interconnexion : répéteur (*transceiver*), concentrateur (*hub*), commutateur (*switch*), routeur (*router*).
- un navigateur, un client de messagerie, un serveur web, ... et une pile de protocoles.

Types de réseaux : par portée

Les réseaux informatiques peuvent être classés suivant leur portée :

- Les réseaux locaux ou **LAN** (*Local Area Network*) correspondent aux réseaux intra-entreprise (quelques centaines de mètres et n'exèdent pas quelques kilomètres), généralement réseaux dits "privés". Le réseau de votre établissement est un réseau de type LAN.
- Les réseaux grandes distances ou **WAN** (*Wide Area Network*) sont des réseaux étendus, généralement réseaux dits "publics" (gérés par des opérateurs publics ou privés), et qui assurent la transmission des données sur des longues distances à l'échelle d'un pays ou de la planète. Internet est un réseau de type WAN.
- Autres dénominations connues : MAN (*Metropolitan Area Network*), PAN (*Personal Area Network*), WPAN et WLAN (*Wireless* ...), SAN (*Storage Area Network*), ...

Frères des Ecoles Chrétiennes
Saint-Jean-Baptiste de la Salle - Avignon

Types de réseaux : par utilisation

Les réseaux informatiques peuvent être classés en fonction de leurs utilisations et des services qu'ils offrent.
Ainsi, pour les réseaux utilisant la famille des protocoles TCP/IP, on distingue :

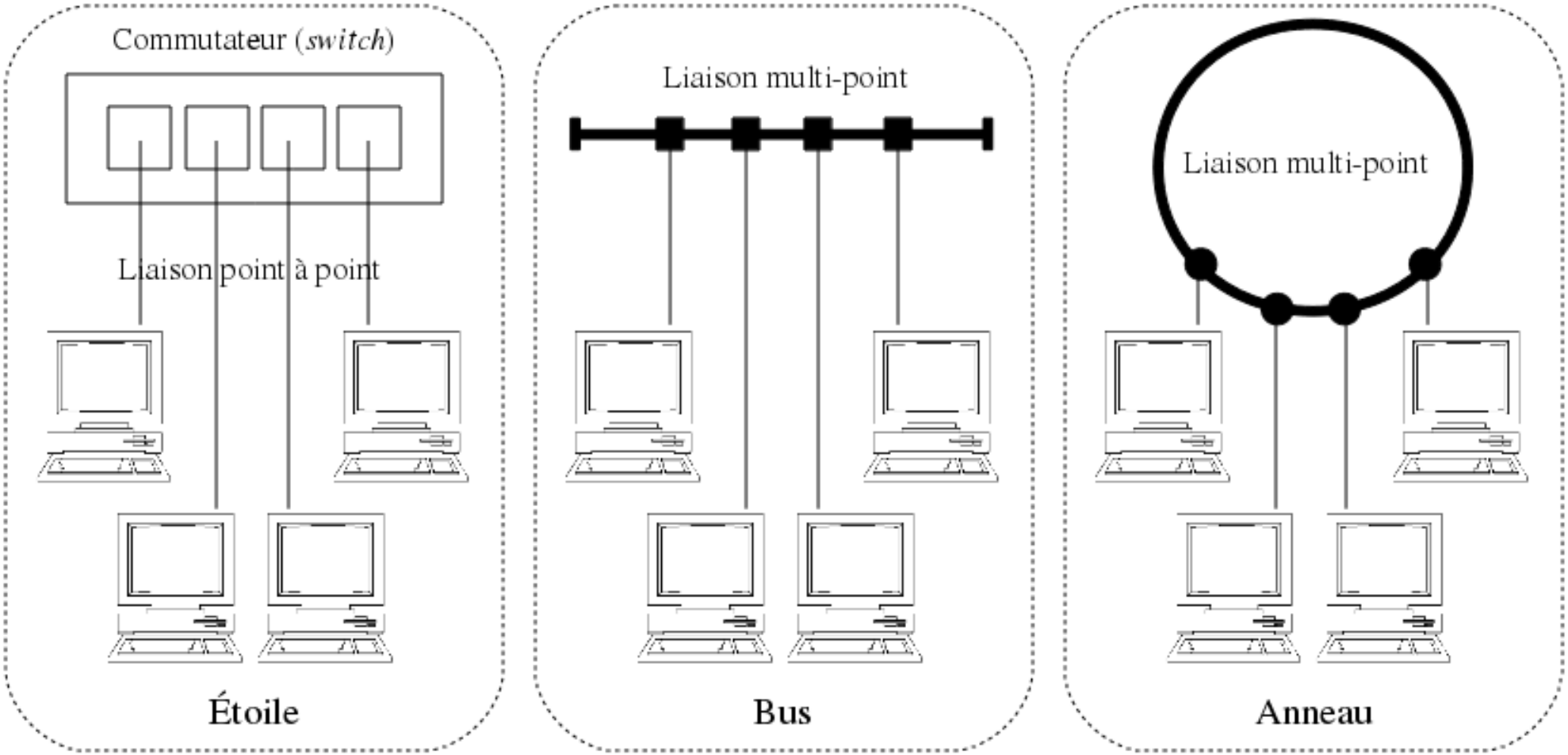
- **Intranet** : le réseau interne d'une entité organisationnelle
- **Extranet** : le réseau externe d'une entité organisationnelle
- **Internet** : le réseau des réseaux interconnectés à l'échelle de la planète

Types de réseaux : par topologie

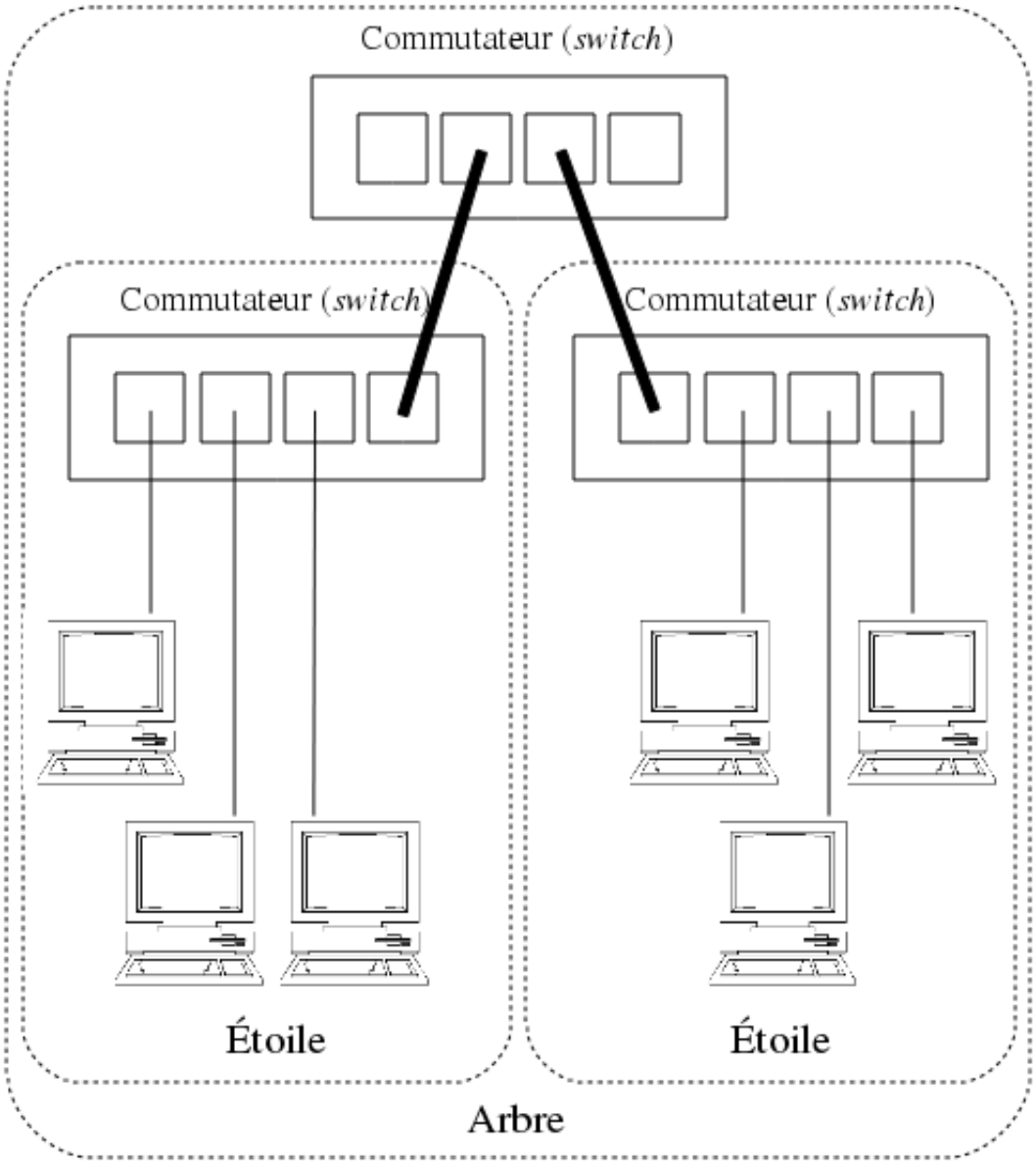
Ils peuvent également être catégorisés par topologie de réseau :

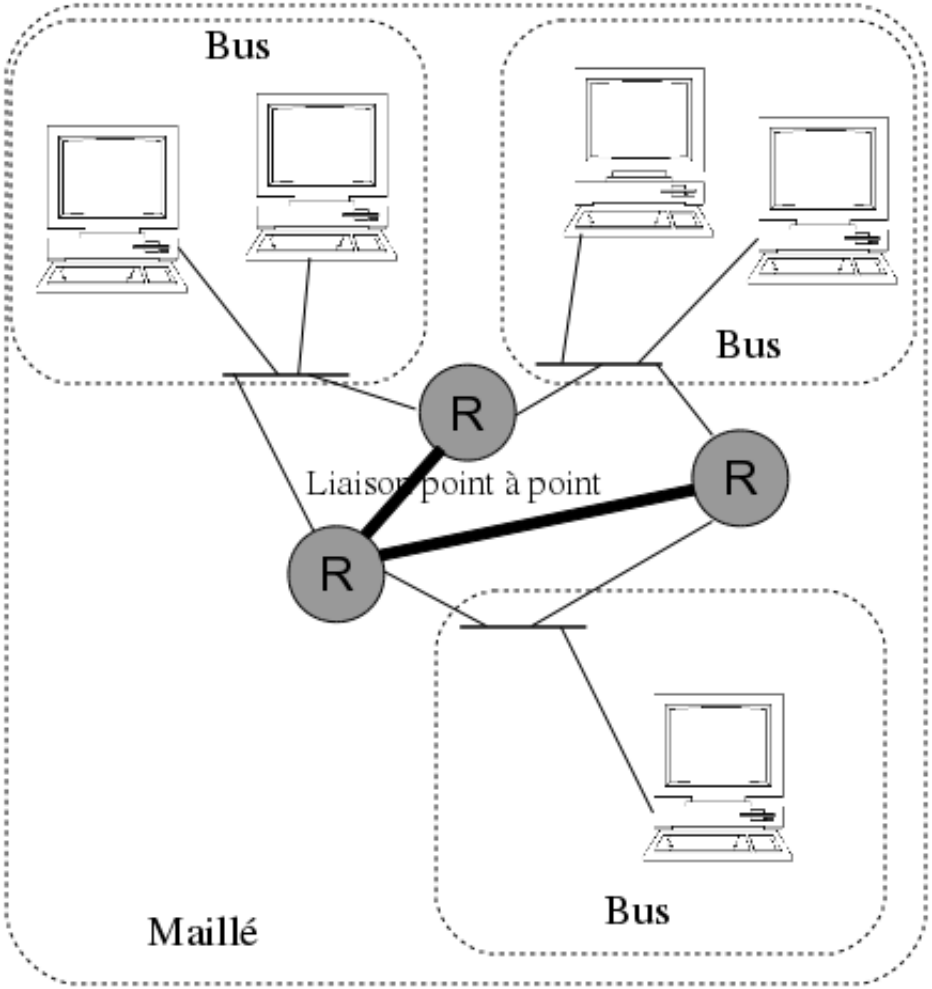
- **Réseau en étoile** : les équipements du réseau sont reliés à un équipement central. En pratique, l'équipement central peut être un concentrateur (*hub*), un commutateur (*switch*) ou un routeur (*router*).
- **Réseau en bus** : l'interconnexion est assurée par un média partagé entre tous les équipements raccordés.
- **Réseau en anneau** : les équipements sont reliés entre eux par une boucle fermée.
- **Réseau en arbre** : souvent un réseau en étoile réparti sur plusieurs niveaux (étoile étendue).

Exemples de topologies



Topologies hybrides



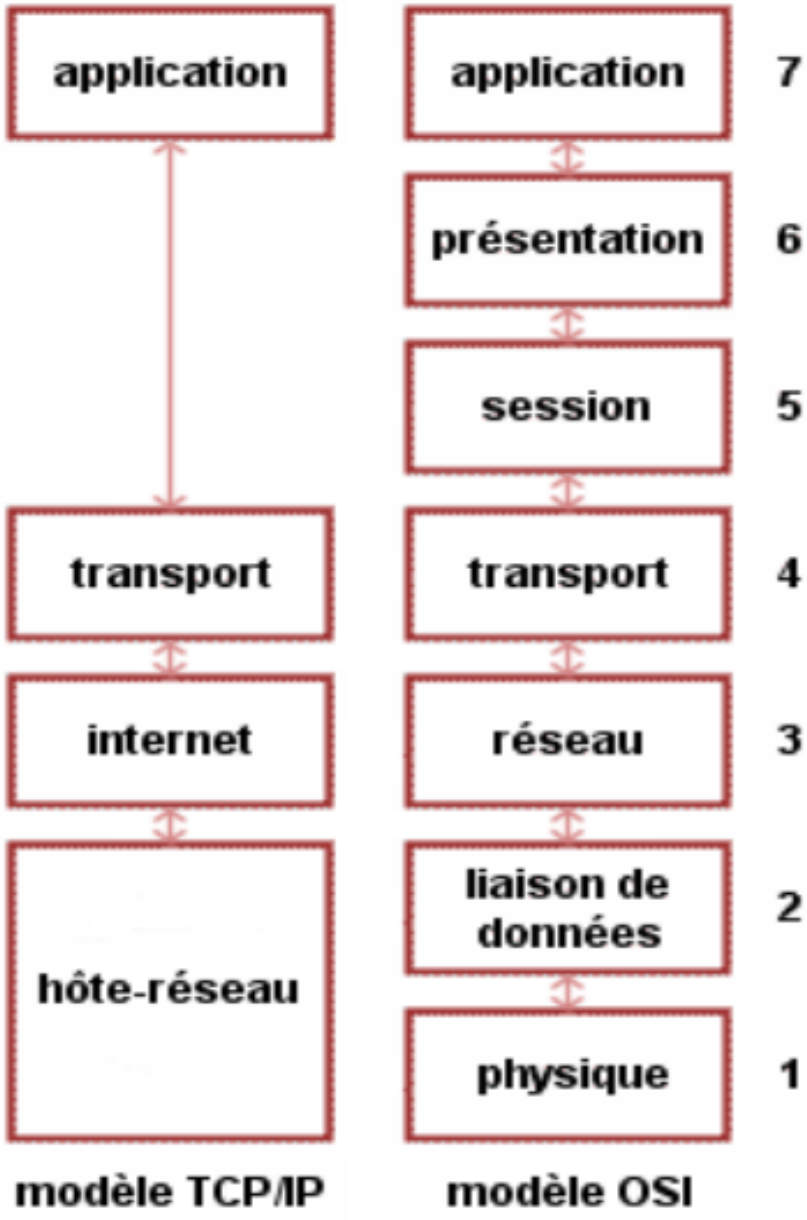


Modèles de référence

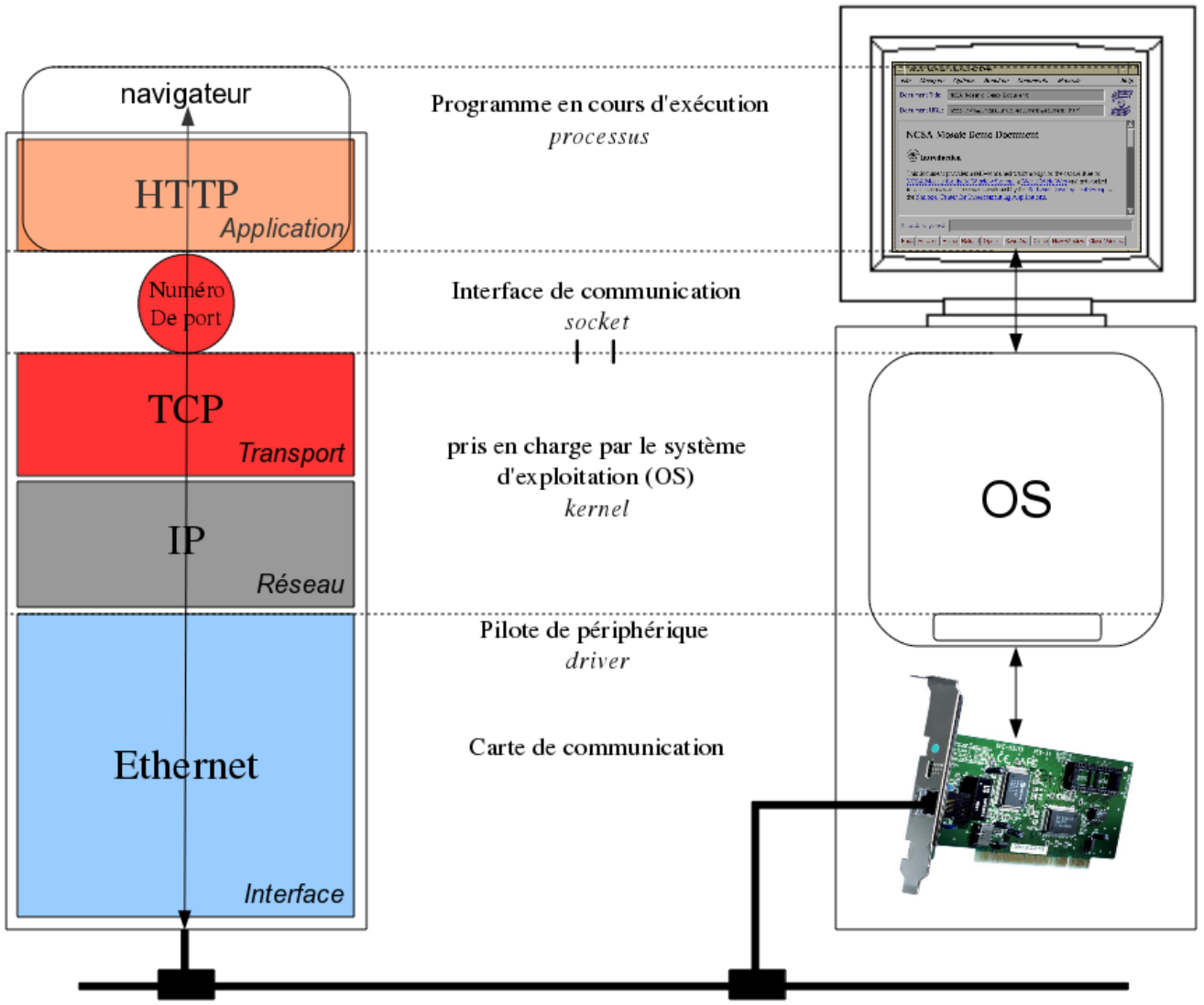
Un **modèle de référence** est utilisé pour décrire la structure et le fonctionnement des communications réseaux.
On connaît deux modèles :

- Le **modèle OSI** (*Open Systems Interconnect*) qui correspond à une approche plus théorique en décomposant le fonctionnement en une **pile de 7 couches**.
- Le **modèle DoD** (*Department Of Defense*) qui répond à un problème pratique comprenant une **pile de 4 couches** pour décrire le réseau Internet (la famille des protocoles TCP/IP).

Modèles OSI et DoD



Le modèle DoD en action



Les couches basses

Dans le modèle OSI, les trois couches basses assurent des fonctions orientées "transmission" :

- La **couche physique** décrit les caractéristiques physiques de la communication, comme le média utilisé (câbles cuivre, fibre optique ou radio), et tous les détails associés comme les connecteurs, les types de codage, le niveau des signaux, ... et les distances maximales. Elle assure la transmission des bits de la trame de la couche supérieure sur le réseau physique.
- La **couche de liaison de données** spécifie comment les paquets de la couche supérieure seront transportés. Elle assure la mise en trames, leurs acheminements sans erreurs et la méthode d'accès au réseau physique.
- La **couche réseau** résout le problème de l'acheminement des paquets à travers un réseau. Elle permet de transférer des données pour de nombreux protocoles de plus haut niveau.

Les couches hautes

Dans le modèle OSI, les couches hautes réalisent des fonctions orientées "traitement" (certaines couches peuvent être vides) :

- La **couche transport** est responsable du transport des données de bout en bout (c'est-à-dire de processus à processus) au travers du réseau.
- La **couche session** établit une communication entre émetteur et récepteur en assurant l'ouverture et la fermeture des sessions.
- La **couche présentation** met en forme les informations échangées pour les rendre compatibles avec l'application destinatrice, dans le cas de dialogue entre systèmes hétérogènes. Elle peut comporter des fonctions de traduction, de compression, d'encryptage, ...
- La **couche application** va apporter les services de base offerts par le réseau pour les logiciels "applicatifs".

Définition

Les équipements d'interconnexion de réseaux permettent :

- de **relier des réseaux hétérogènes** (couches et protocoles différents)
- d'**organiser au mieux le réseau** pour une exploitation optimale (adressage des réseaux et sous-réseaux, *VLAN*, *proxy*, ...)
- de **contourner les limites techniques** des architectures des réseaux (augmentation des distances des segments physiques, changement de support physique, ...)
- d'**offrir une sécurité maximale** (parefeu ou *firewall*, *VLAN*, *proxy*, ...)

Niveau 1 : couche physique

Le **répéteur** (*transceiver*) est un équipement d'interconnexion de niveau 1 qui assure la répétition des bits d'un segment sur l'autre (régénération du signal pour compenser l'affaiblissement) et qui permet :

- d'**augmenter la distance d'un segment physique**
- **le changement du support physique**

Le **concentrateur** (*hub*) est aussi un équipement d'interconnexion de niveau 1 qui interconnecte les équipements sur le même réseau physique. Le *hub* se comporte comme un **répéteur multi-ports**. En *Ethernet* avec un *hub* 100Mbps, on obtient un débit partagé de 100Mbps pour l'ensemble des équipements raccordés. Même si la topologie physique est en étoile, un réseau *Ethernet* constitué d'un *hub* suit une topologie logique en bus.

La trame n'est jamais modifiée lors de la traversée d'un répéteur ou d'un concentrateur (*hub*).

Niveau 2 : couche liaison

Le **pont** (*bridge*) et le **commutateur** (*switch*) sont des équipements d'interconnexion de niveau 2 qui relient des équipements appartenant à un même réseau physique (LAN). Unique différence, le commutateur ne convertit pas les formats de transmissions de données. Sinon, ces deux équipement sont capables :

- d'**analyser les trames** qui circulent sur chaque segment pour stocker et mettre à jour périodiquement la table de correspondance adresse physique/n°de port
- de **filtrer les trames en fonction de l'adresse physique du destinataire** (segmentation de réseaux physiques)
- d'**assurer les fonctions d'un répéteur**

En *Ethernet* avec un *switch* 100Mbps, on obtient un débit dédié de 100Mbps par port. Un réseau *Ethernet* constitué d'un *switch* suit une topologie physique et logique en étoile.

VLAN (*Virtual LAN*)

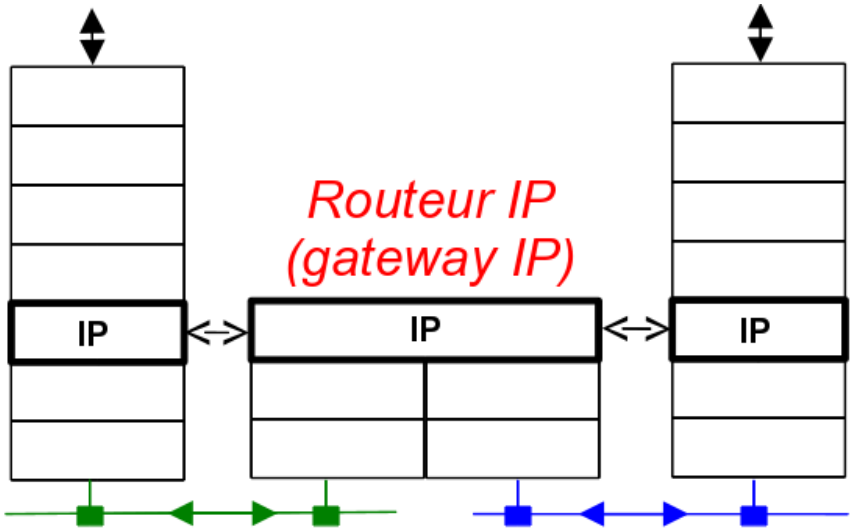
Un **réseau virtuel**, appelé **VLAN** (*Virtual LAN*), est un **réseau logique indépendant de niveau 2**. De nombreux *VLAN* peuvent coexister sur un même commutateur (*switch*).
Les VLAN permettent :

- la **segmentation** en réduisant la taille d'un domaine de diffusion (*broadcast*)
- la **flexibilité** en filtrant les adresses MAC du niveau 2 (couche liaison) voire jusqu'au niveau 3 (IP)
- la **sécurité** en permettant de créer un ensemble logique isolé. Le seul moyen pour communiquer entre des *VLAN* différents sera alors de passer par un routeur.

L'administrateur crée un *VLAN* en affectant un port à un *VLAN* (*Port-based VLAN*) ou en utilisant une adresse MAC de niveau 2 ou éventuellement une adresse IP de niveau 3.

Niveau 3 : couche réseau

Le **routeur** (*router*) est un équipement d'interconnexion de niveau 3 qui permet d'**acheminer des paquets d'un réseau logique vers un autre**.



Le routeur doit posséder une adresse IP dans chaque réseau IP qu'il interconnecte. On dit qu'il est multi-domicilié.

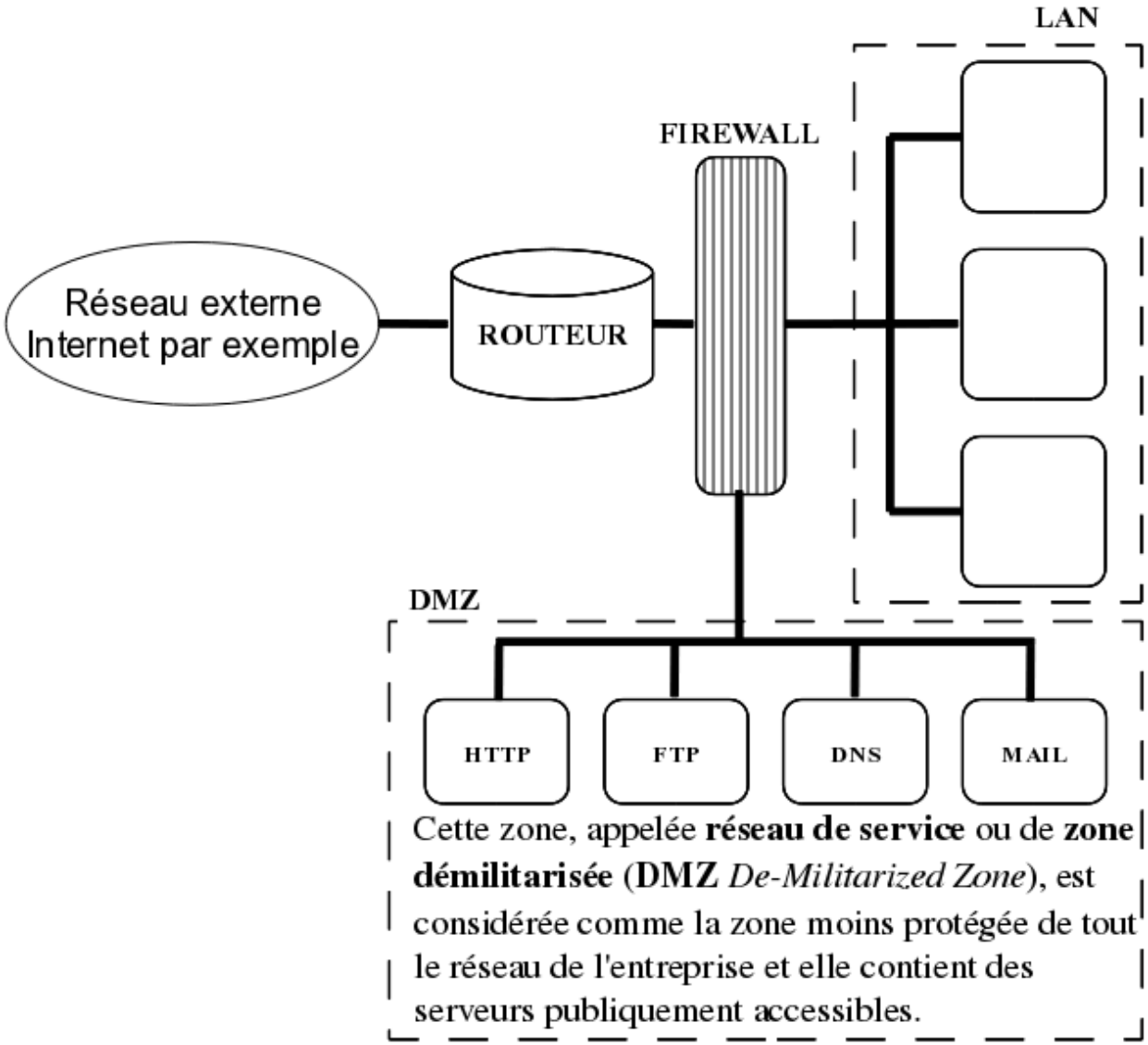
Un routeur moderne se présente comme un boîtier regroupant carte mère, microprocesseur, mémoire ROM, RAM ainsi que les ressources réseaux nécessaires (Wi-Fi, Ethernet, ...). On peut donc le voir comme un ordinateur minimal dédié, dont le système d'exploitation est très souvent un *Linux* allégé.

Pare-feu (*firewall*)

Un système pare-feu (*firewall*) est un dispositif conçu pour examiner et éventuellement bloquer les échanges de données entre réseaux. C'est donc un **élément de sécurité**. Le pare-feu joue le rôle de filtre et peut donc intervenir à plusieurs niveaux du modèle DoD ou OSI en analysant les en-têtes des protocoles. Il existe trois types principaux de pare-feu :

- Le **filtrage de paquets** basé sur les adresses source et destination, les protocoles et surtout les numéro de ports
- Le **filtrage de paquets avec état** (*firewall stateful*) qui assure un suivi de session et de connexion
- Le ***proxy*** qui intervient jusqu'à la couche application

DMZ (*De-Militarized Zone*)



Serveur mandataire ou *proxy*

Un serveur mandataire ou *proxy* est un serveur qui a pour fonction de **relayer des requêtes entre un poste client et un serveur d'application**. Les serveurs *proxy* sont notamment utilisés pour assurer les fonctions suivantes :

- l'accélération des performances : mise en mémoire cache, compression des données, ...
- la journalisation des requêtes (« *log* »)
- le filtrage et l'anonymat
- l'authentification pour autoriser ou non l'accès au service

Il est presque systématique en entreprise ou dans les établissements scolaires que l'accès internet se fasse à travers un serveur *proxy*.

Saint-Jean-Baptiste de la Salle - Avignon

Définition

Les échanges de données entre équipements sont basés sur une **communication logique** qui se définit par les principes généraux suivants :

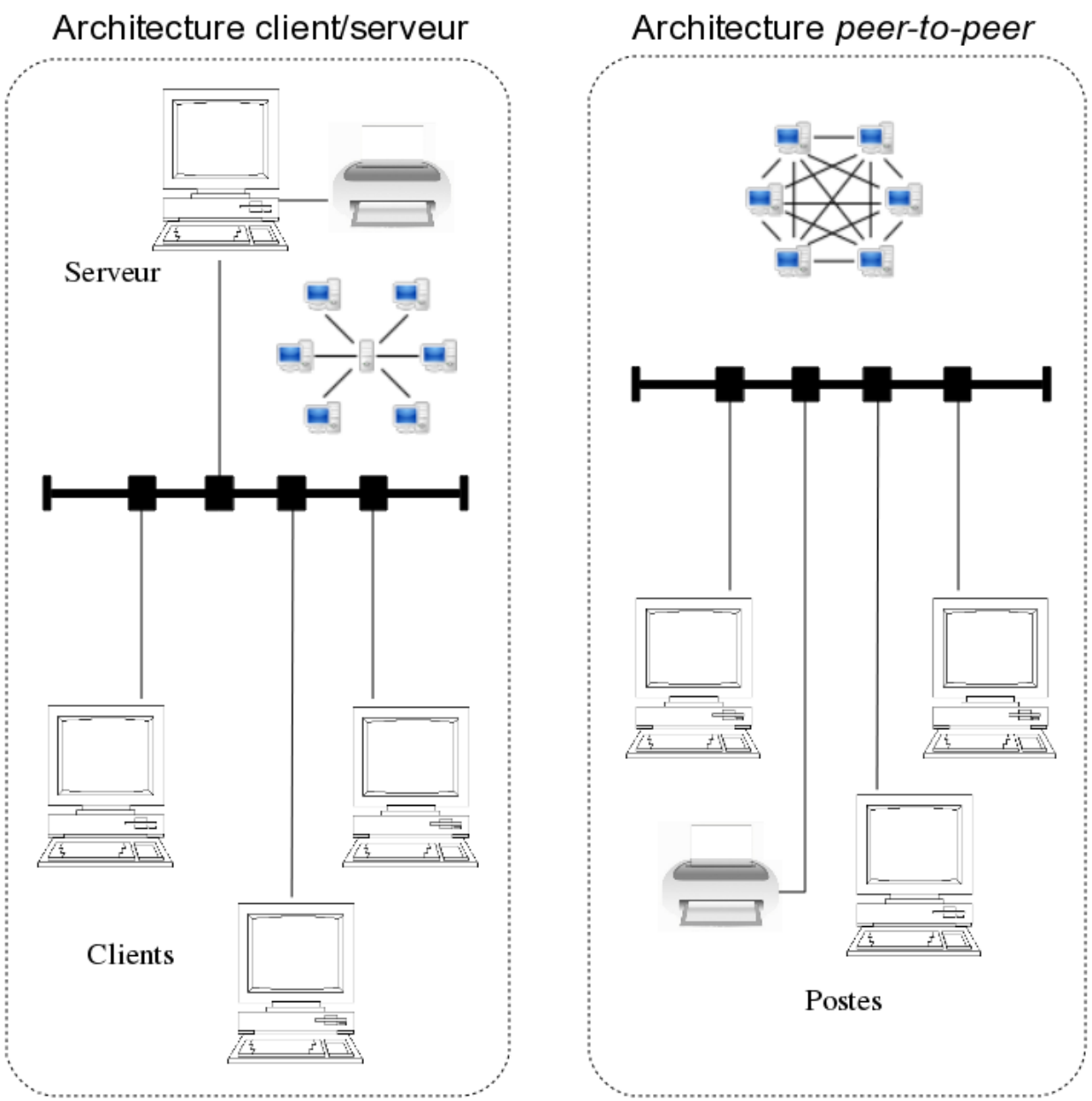
- L'**architecture** qui définit les rôles endossés par les équipements.
- Les **protocoles** qui assurent l'échange des données.
- L'**adressage** qui permet d'identifier de manière unique les équipements en communication.

Catégories

Les réseaux informatiques peuvent aussi être catégorisés par la relation fonctionnelle (le "rôle") entre les équipements.
On distingue par exemple :

- L'architecture **client/serveur** qui centralise des ressources sur un **serveur** qui offre des **services** pour des **clients**. Le réseau Internet, basé sur cette architecture, peut être vu comme un **réseau de services** composés exclusivement de **serveurs**.
- L'architecture **poste à poste ou pair-à-pair** (*peer-to-peer*) qui permet de partager simplement des fichiers le plus souvent, mais aussi des flux multimédia continus (*streaming*) ou du calcul réparti. Les systèmes *peer-to-peer* permettent une décentralisation des systèmes, en permettant à tous les ordinateurs de jouer le rôle de client et de serveur.

Les architectures client/serveur et peer-to-peer



L'architecture client/serveur

L'architecture **client/serveur** désigne un mode de communication à travers un réseau entre plusieurs programmes ou logiciels :

- Le processus **client envoie des requêtes pour demander un service**.
- Le processus **serveur attend les requêtes des clients et y répond en offrant le service**.

La communication s'initie TOUJOURS à la demande du client.

Par extension, le client désigne également l'ordinateur sur lequel est exécuté le logiciel (processus) client, et le serveur, l'ordinateur sur lequel est exécuté le logiciel (processus) serveur.

Définition

Les protocoles rendent possible le dialogue entre des machines différentes en définissant les **règles pour réaliser une communication**.
Cela comprend :

- Le **dictionnaire** : la liste des primitives (comme demande connexion, acquittement, ...)
- Le **scénario** du dialogue : l'enchaînement des primitives (représentable par un diagramme de l'échange)
- Les **modalités** : la taille et la représentation des informations, temps d'attente, etc ...
- Les **messages** échangés : les différents champs composant le bloc d'informations (taille et contenu)

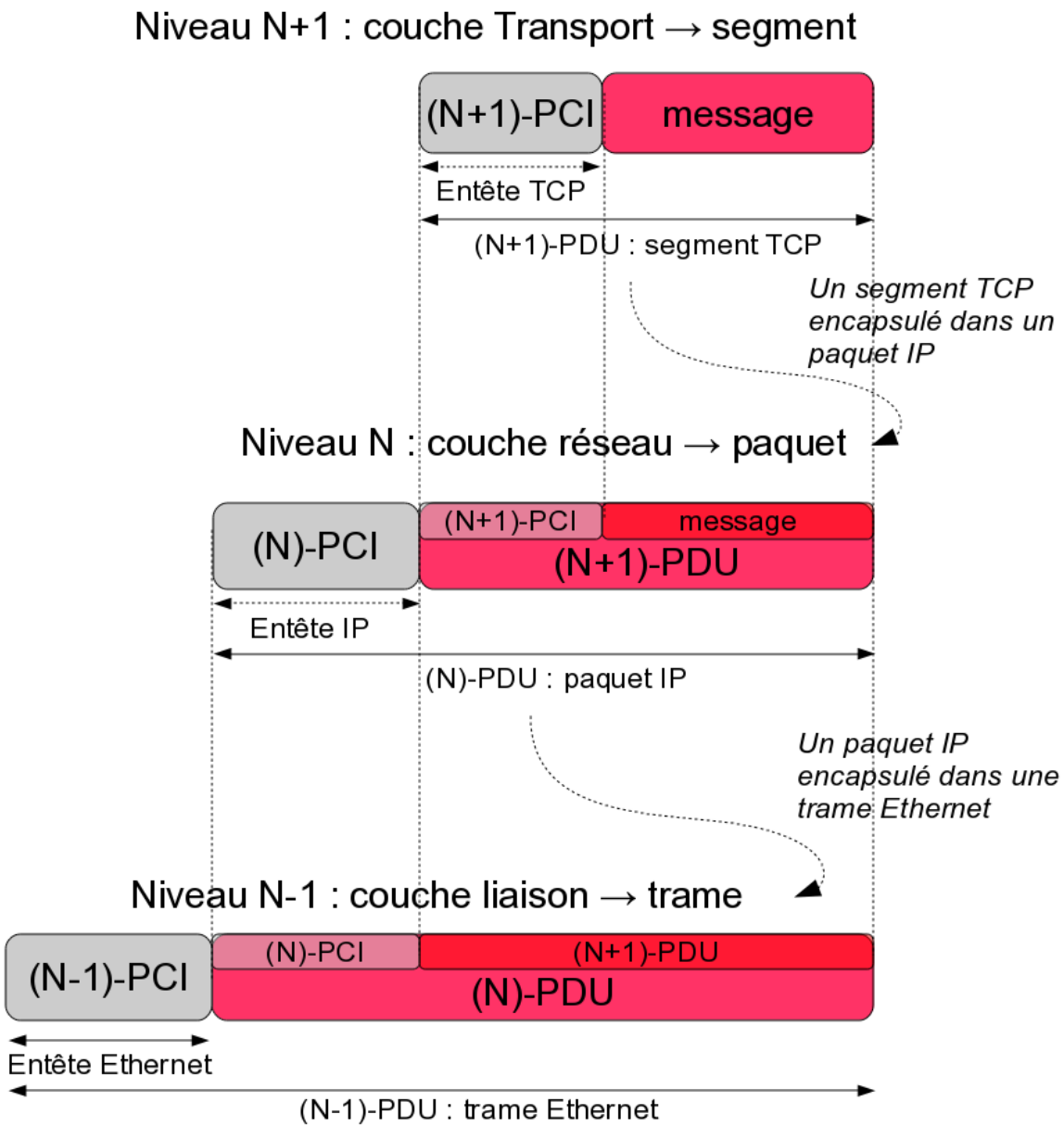
Principe

Le bloc d'informations défini par un protocole réseau est constitué de deux parties :

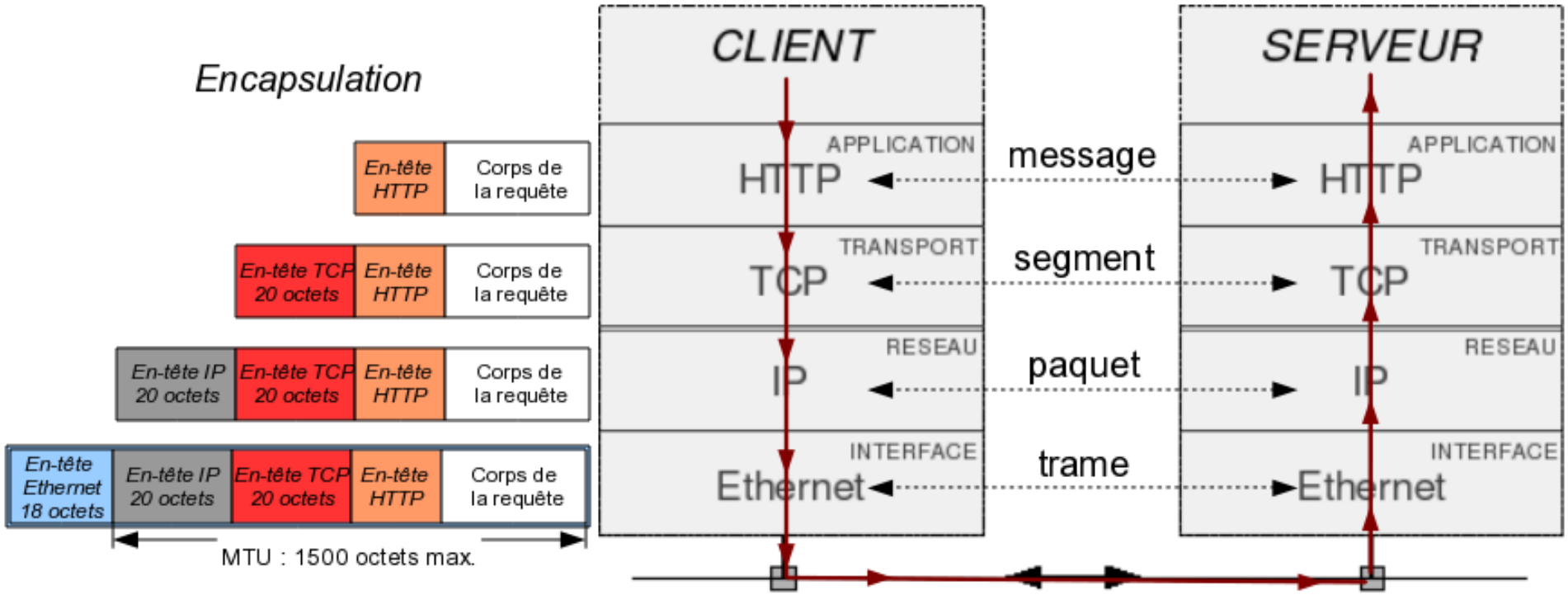
- un **PCI** (*Protocol Control Information*) : les informations propres au protocole utilisé. On utilise souvent le terme d'**entête** de protocole (*header*).
- un **PDU** (*Protocol Data Unit*) : les données "réseau" transportées, qui réprésente un bloc de la couche supérieure.

Attention, il ne faut confondre les données "réseau" (un PDU) avec les données "utilisateur". Cela est dû à l'encapsulation des protocoles du modèle de référence utilisé.

L'encapsulation



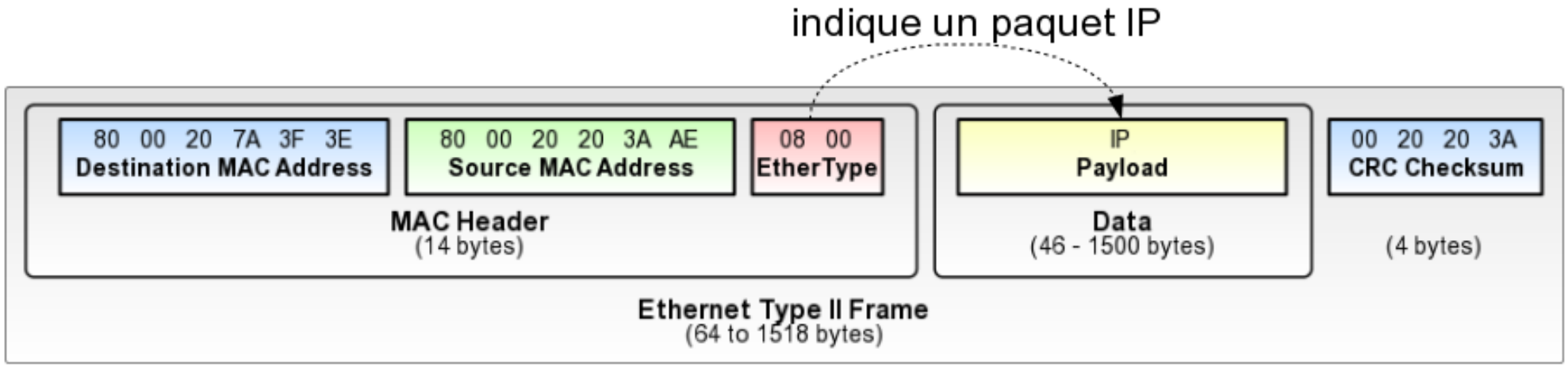
Exemple



Le protocole HTTP (*HyperText Transfer Protocol*) de la couche Application est utilisé dans les communications du service web (*World Wide Web*).

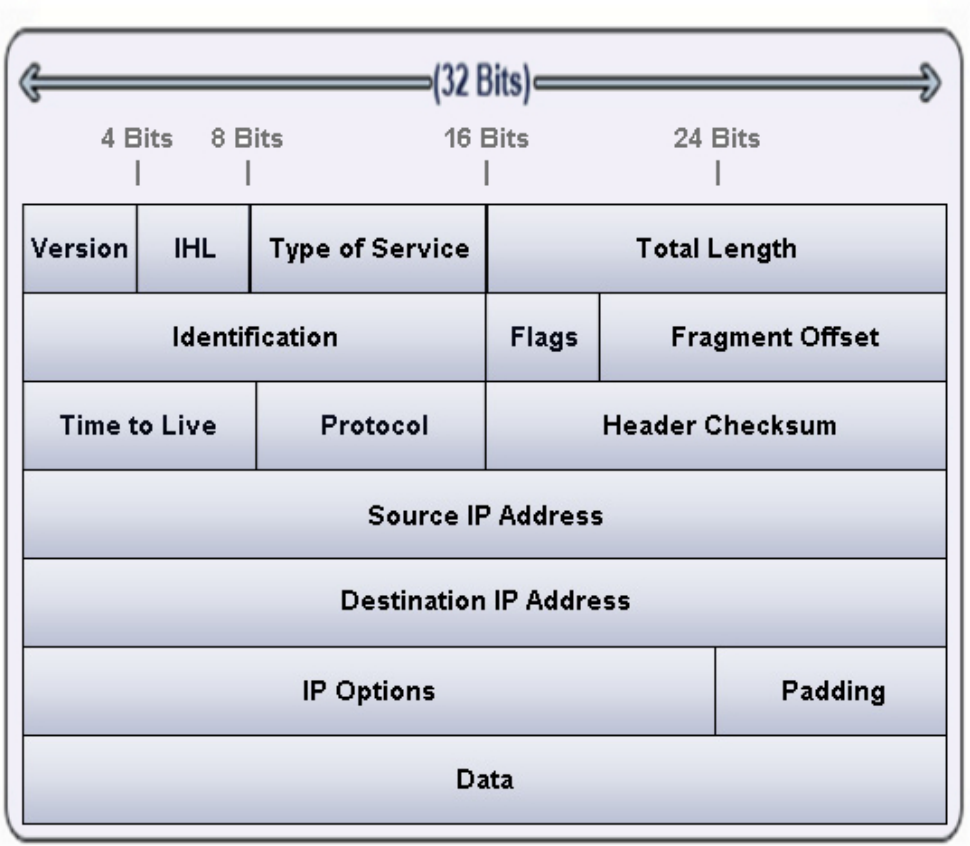
Le protocole Ethernet_II

Ethernet_II représente le type de trame le plus utilisé actuellement par le protocole de réseau local *Ethernet*. Cette trame transporte le plus souvent un paquet IP.



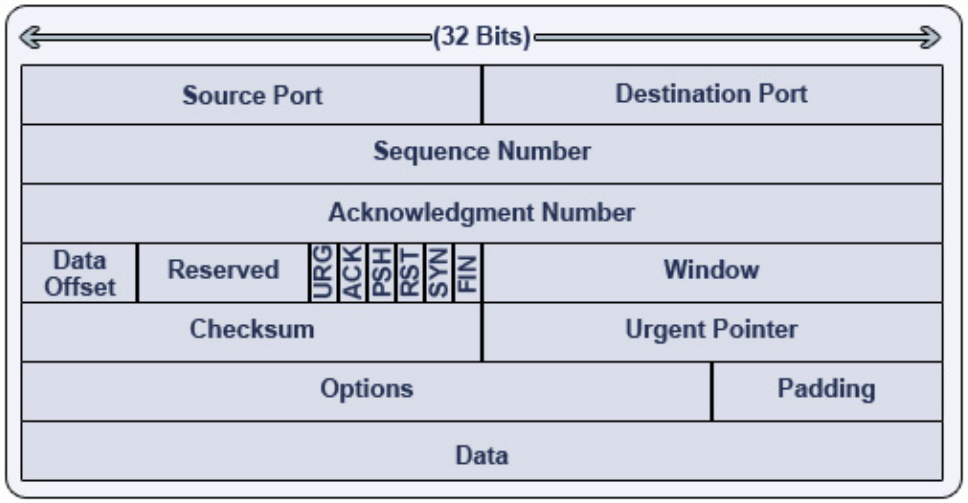
Le protocole IPv4

IPv4 (*Internet Protocol version 4*) représente le protocole réseau le plus répandu actuellement. Il permet de découper l'information à transmettre en paquets, de les adresser, de les transporter indépendamment les uns des autres et de recomposer le message initial à l'arrivée.



Le protocole TCP

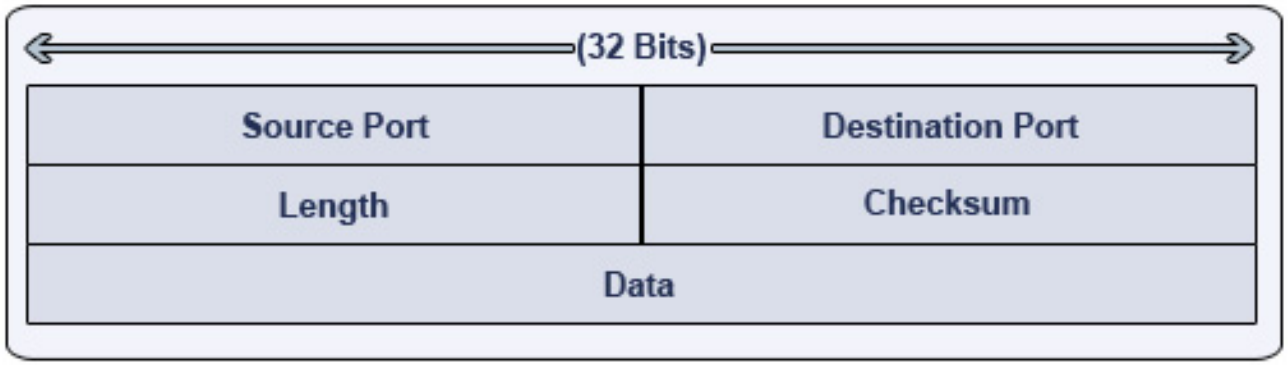
TCP (*Transmission Control Protocol*) est un protocole de transport complexe donc lent mais fiable, utilisé en **mode connecté** qui assure la transmission des données de bout en bout (d'un processus à un autre processus).



Le mode connecté ne permet pas au protocole TCP d'être utilisé pour des communications un-vers-tous (*broadcast*) ou un-vers-plusieurs (*multicast*). Seules les communications de type un-vers-un (*unicast*) peuvent être réalisées.

Le protocole UDP

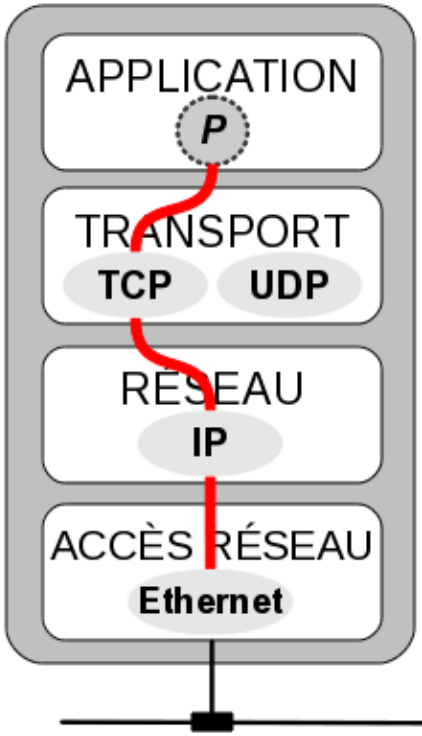
UDP (*User Datagram Protocol*) est un protocole simple donc rapide mais décrit comme étant non-fiable, utilisé en **mode non-connecté** qui assure la transmission des données de bout en bout d'un processus à un autre processus.



Le mode non connecté permet au protocole UDP d'être utilisé pour des communications un-vers-un (*unicast*), un-vers-tous (*broadcast*) et un-vers-plusieurs (*multicast*).

En résumé

La famille des **protocoles TCP/IP** étant la plus répandue à l'heure actuelle, la "compréhension générale" d'un réseau informatique peut être résumée de la façon suivante :



La couche APPLICATION permet l'accès à un service du réseau. Un processus est un programme qui s'exécute sur l'équipement et qui utilise un des nombreux protocoles de cette couche pour accéder à un service : si c'est un client, il émettra une demande de service (requête) et si c'est un serveur, il offrira le service demandé (réponse).

La couche TRANSPORT est responsable du transport des données de bout en bout entre processus. TCP (*Transmission Control Protocol*) est un protocole de transport, en mode connecté, lent mais fiable. UDP (*User Datagram Protocol*) est un protocole de transport, en mode non connecté, simple et rapide mais peu fiable.

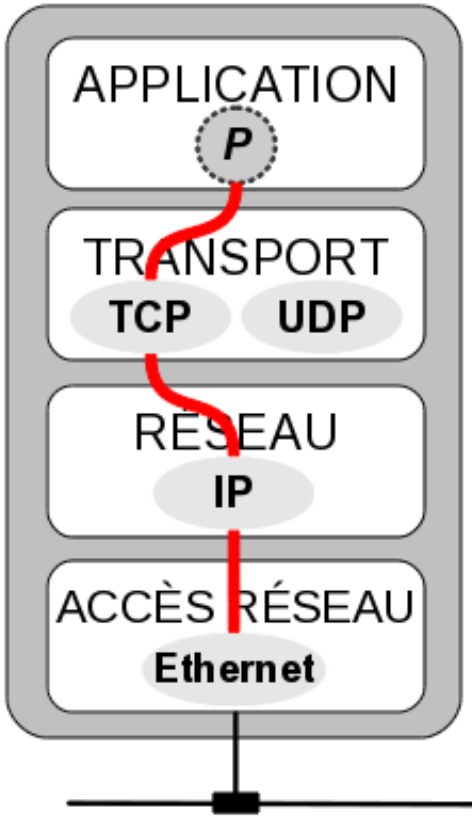
La couche RÉSEAU assure l'acheminement des paquets à travers un réseau de noeuds en noeuds jusqu'à la machine destinatrice. IP (*Internet Protocol*) est un protocole fournissant une méthode pour mener les paquets à destination en intégrant un service d'adressage unique pour l'ensemble des équipements.

La couche ACCÈS RÉSEAU (ou Interface) spécifie comment les paquets sont transportés sur le réseau physique. Ethernet est un protocole de réseau local qui permet l'émission et la réception de paquets dans des trames.

Frères des Ecoles Chrétiennes Saint-Jean-Baptiste de la Salle - Avignon

Vue générale

Les **adresses** forment une notion importante en communication et sont un **moyen d'identification**. Dans un réseau informatique, on distinguera :



Chaque protocole de cette couche peut posséder un adressage particulier associé à son service. On peut citer par exemple l'adressage par *URL* pour le service *web* ou l'adresse *email* pour le service messagerie.

On utilise un **numéro de port** pour identifier un processus client ou serveur de la couche APPLICATION. Pour les serveurs, il existe des numéros de port *bien connus*.

On utilise des **adresses IP** pour identifier de manière unique l'équipement sur le réseau logique. Chaque interface de l'équipement doit posséder une adresse IP.

On utilise des **adresses MAC** pour identifier de manière unique l'interface sur le réseau physique.

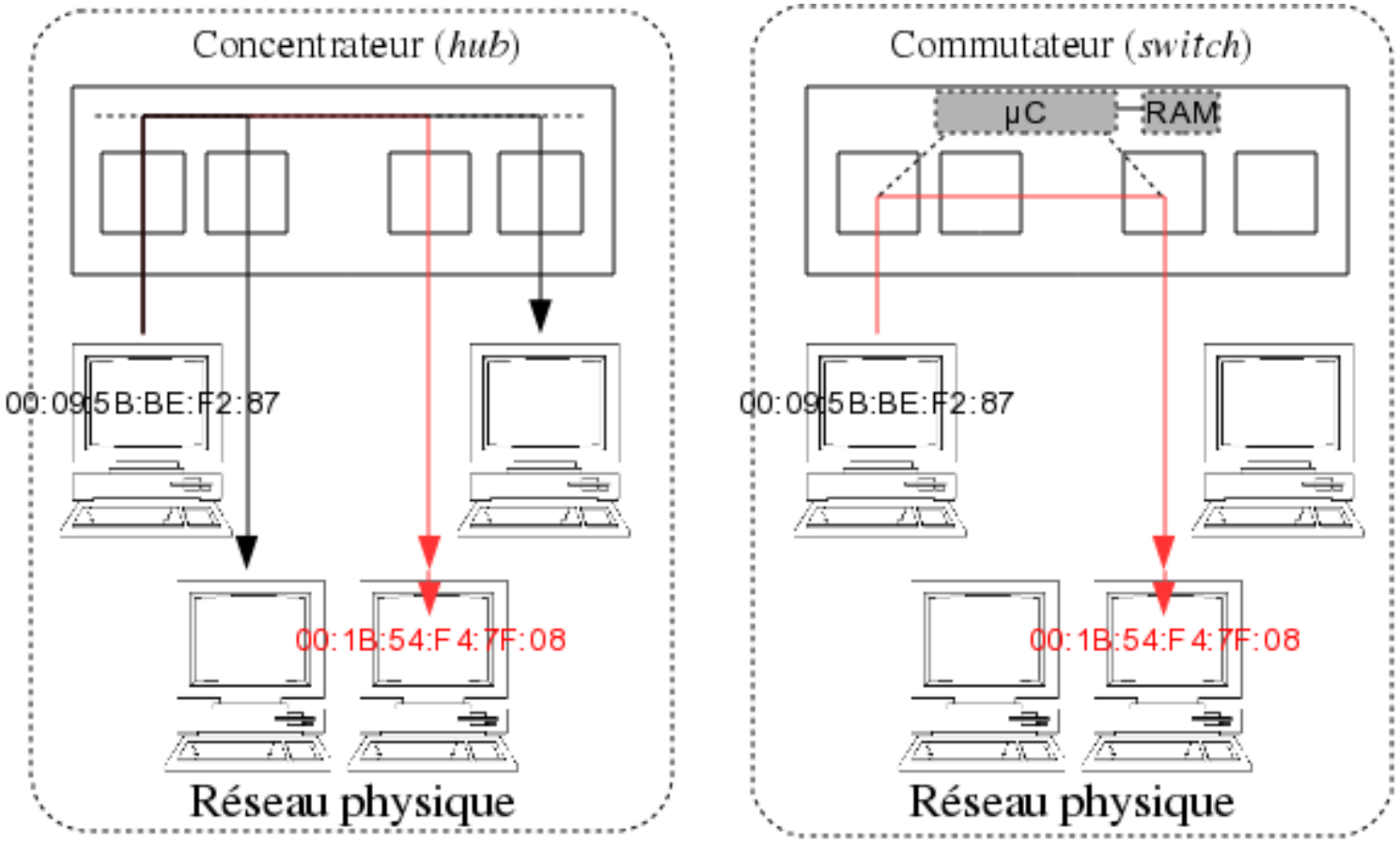
L'adressage physique

L'adressage physique utilise une **adresse matérielle** (appelée généralement **MAC**) qui permet d'**identifier de manière unique l'interface de communication d'un équipement sur un réseau physique**.
Les **adresses MAC** :

- sont utilisées dans les **entêtes des trames de la couche Liaison afin d'identifier l'émetteur et le destinataire**.
- sont codées sur **48 bits soit 6 octets** (les trois 3 premiers octets permettent d'identifier le fabricant de l'interface de communication).
- ne donnent aucune indication sur la situation "géographique" de l'équipement et donc ne permet pas une organisation optimale du réseau. Cette faiblesse sera compensée par un adressage logique au niveau de la couche Réseau.

Frères des Ecoles Chrétiennes Saint-Jean-Baptiste de la Salle - Avignon

Réseaux physiques



Le concentrateur et le commutateur sont les équipements qui permettent de constituer un réseau physique.

L'adressage logique

L'**adressage logique** intervient au niveau de la couche Réseau afin d'**identifier un équipement dans un réseau**. L'adressage logique le plus utilisé actuellement est l'**adressage IP**.
Les **adresses IP** :

- sont utilisées dans les **entêtes des paquets afin d'identifier l'émetteur et le destinataire**.
- sont codées sur **32 bits (pour la version 4)** et sur 128 bits (pour la version 6).
- utilisent une **notation décimale pointée** pour la version 4 qui est encore la plus utilisée actuellement : quatre nombres, compris entre 0 et 255, séparés par des points (exemple : 212.85.150.134).
- sont décomposables en deux parties en utilisant un **masque** :
  - le *netid* qui identifie le réseau auquel appartient l'hôte
  - le *hostid* qui identifie le numéro de l'hôte dans ce réseau.

Frères des Ecoles Chrétiennes Saint-Jean-Baptiste de la Salle - Avignon

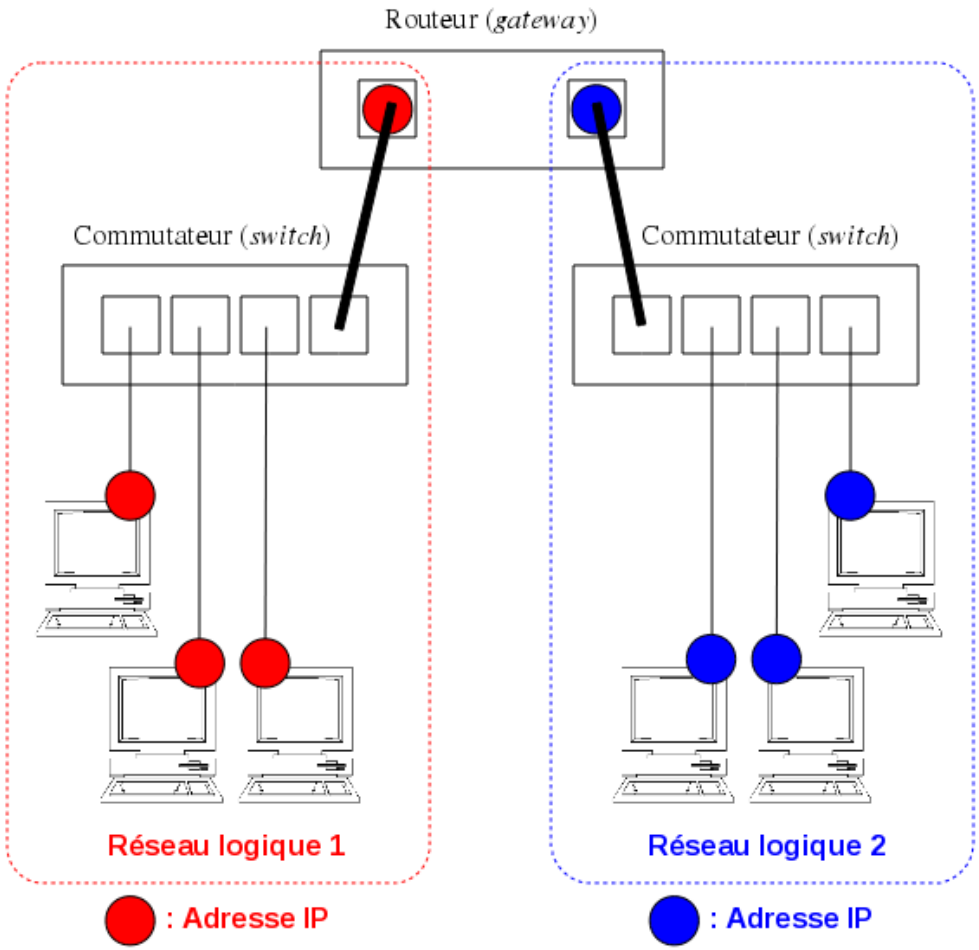
Notion de masque

Pour décomposer une adresse IP (c'est-à-dire séparer le *netid* du *hostid*), il faut utiliser un **masque (*netmask*)**. Chaque équipement effectuera une opération **ET (bit à bit)** entre l'adresse IP complète et le masque.

Il suffit alors de placer des bits à 1 dans le masque pour conserver le *netid* et des 0 pour écraser le *hostid*. Un masque a donc la même longueur qu'une adresse IP.

C'est donc la valeur du masque qui définit le *netid* (et donc le *hostid*). On parle de masque de réseau. La valeur du masque est essentielle dans l'adressage IP. C'est le masque qui définit la taille d'une réseau IP (càd la plage d'adresses assignables aux machines du réseau).

Réseaux logiques



Le routeur est le seul équipement permettant de faire communiquer des réseaux logiques entre eux.

Notion d'échanges directes et indirectes

À partir du schéma précédent, on distingue deux situations :

- Les équipements communiquent directement entre eux à condition qu'ils soient sur le même réseau IP (même *netid*). Ils peuvent être interconnectés physiquement par des concentrateurs (*hub*) et/ou des commutateurs (*switch*).
- Les équipements qui n'appartiennent pas au même réseau IP (*netid* différents) ne peuvent pas communiquer entre eux directement. Ils pourront le faire par l'intermédiaire d'un **routeur (*gateway*)**.

Le routeur doit posséder une adresse IP dans chaque réseau IP qu'il interconnecte. On dit qu'il est multi-domicilié.

Frères des Ecoles Chrétiennes Saint-Jean-Baptiste de la Salle - Avignon

Types d'adresses

On distingue différents techniques d'adressage :

- l'*unicast* désigne **une adresse réseau unique** permettant d'identifier un hôte sur un réseau.
- le *broadcast* permet le transfert d'un hôte vers tous les autres hôtes, en utilisant une adresse spécifique nommée **adresse de *broadcast* (ou adresse de diffusion générale)**.
- le *multicast* permet la communication simultanée avec un groupe d'ordinateurs identifiés par une adresse spécifique nommée **adresse de *multicast* (ou adresse de groupe)**. Les récepteurs intéressés par les messages adressés en *multicast* doivent s'abonner au préalable à ce groupe.
- l'*anycast* désigne une technique où on l'on dispose de plusieurs adresses pour une destination mais une seule sera utilisée.

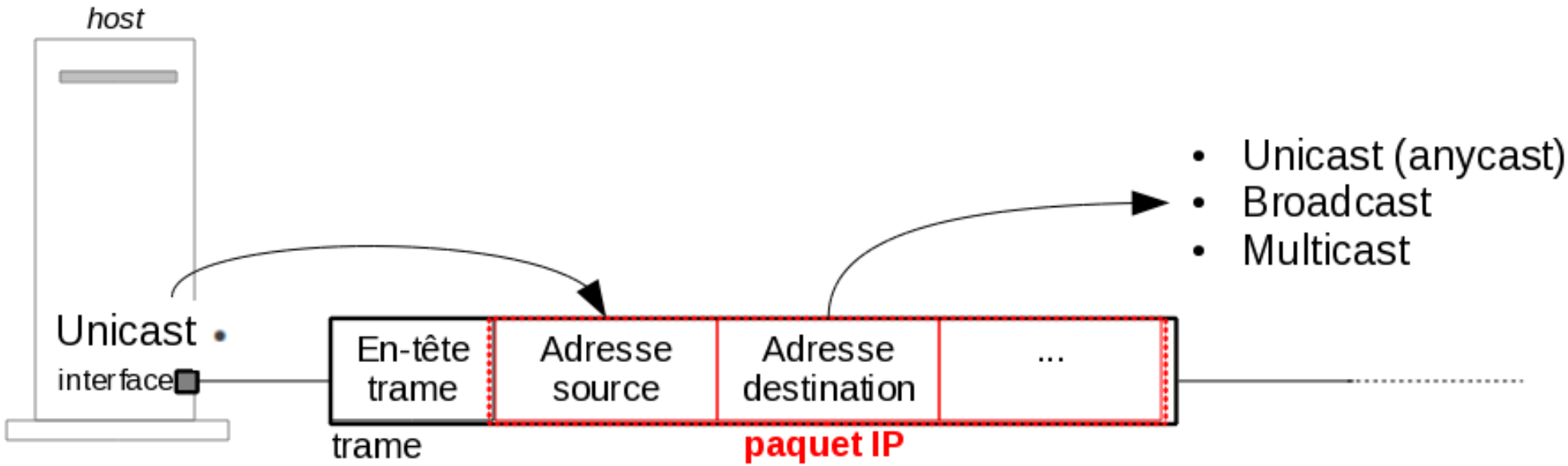
Affectation des adresses IP

On distingue deux situations pour assigner une adresse IP à un équipement :

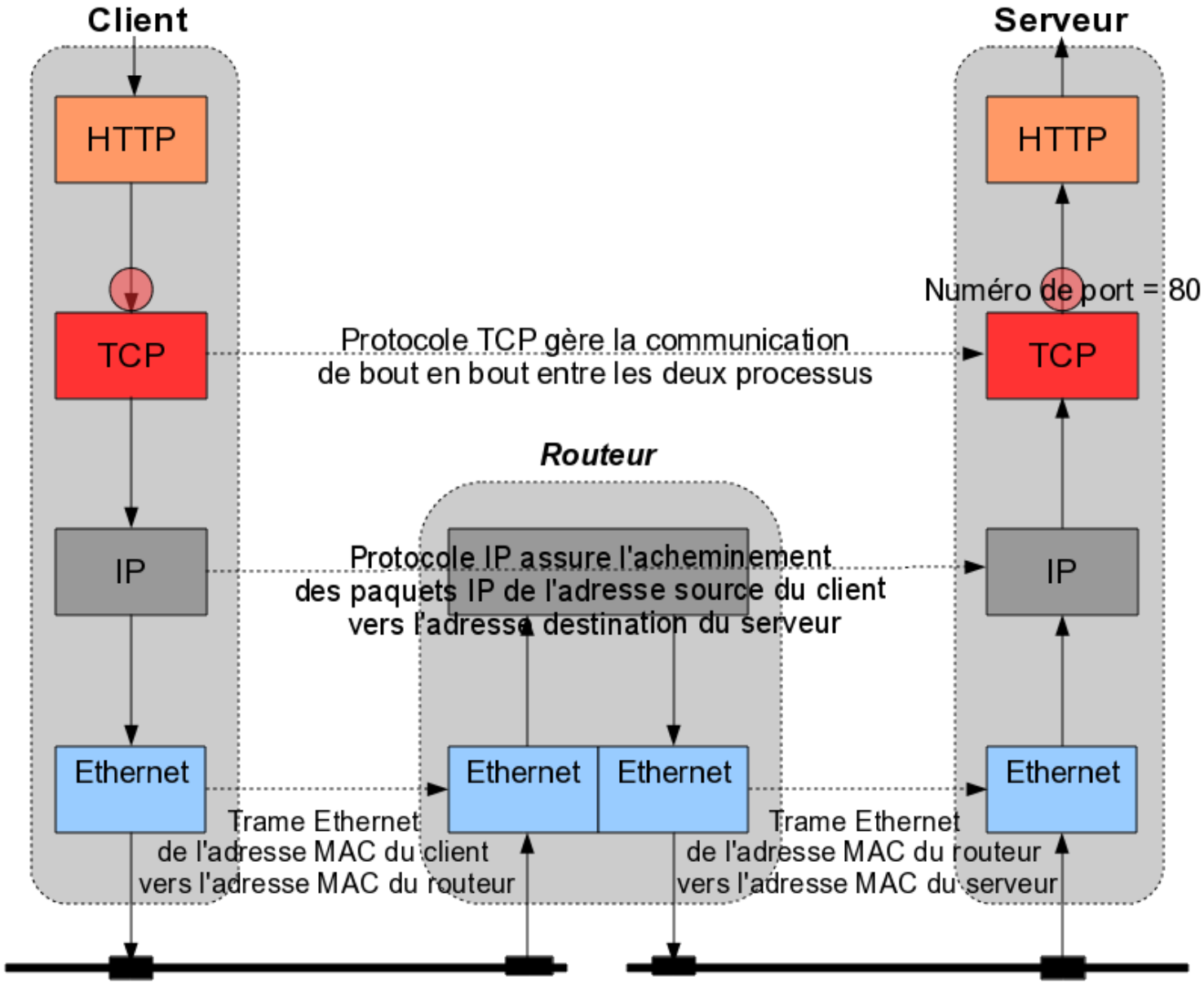
- de manière **statique** : l'adresse est **fixe** et configurée le plus souvent **manuellement** puis stockée dans la configuration de son système d'exploitation.
- de manière **dynamique** : l'adresse est **automatiquement** transmise et assignée grâce au protocole DHCP (*Dynamic Host Configuration Protocol*) ou BOOTP.

Principe

L'adresse *unicast* est la seule adresse utilisable comme **adresse source dans un paquet**.



Adressages physique et logique



Réseaux publics et privés

On doit maintenant distinguer deux types de réseaux adressables en IP :

1. le réseau public **Internet** où chaque équipement connecté doit posséder une adresse unique et enregistrée au niveau mondial.
2. les réseaux privés, dans ce cas le choix des adresses est libre et ne doivent être uniques que dans ce réseau.

Remarques :

- Si un réseau privé doit être interconnecté avec le réseau Internet, il faudra alors utiliser des adresses privées qui ne puissent correspondre à des adresses publiques utilisées sur Internet. Des **plages d'adresses réservées à usage privé** existent et elles ne sont donc pas acheminées par les routeurs Internet, ce qui supprime tout risque de conflit.
- Dans ce cas, pour interconnecter un réseau privé avec Internet, on utilisera un **routeur NAT (*Network Address Translation*)** qui permet de remplacer l'adresse IP source privée par l'adresse publique du routeur.

Frères des Ecoles Chrétiennes Saint-Jean-Baptiste de la Salle - Avignon

Analyseur de protocole

Un **analyseur de protocole** est un **logiciel d'analyse de protocole ou « packet sniffer »** utilisé dans le dépannage et l'analyse de réseaux informatiques, le développement de protocoles, l'éducation et la rétro-ingénierie, mais aussi le piratage.