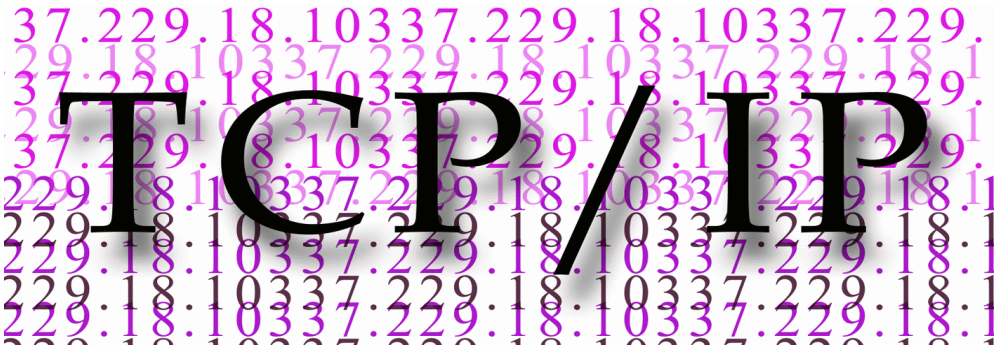
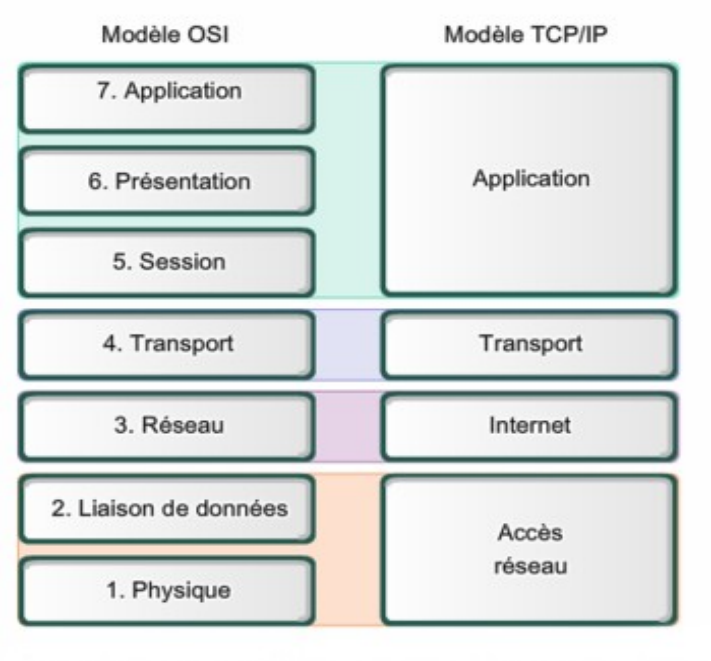
Le Protocole TCP IP



I : Les 4 couches du modèle TCP IP



Définition : le modèle TCP IP est une norme d'échange de données entre ordinateurs. C'est une simplification du modèle OSI en 7 couches sur lequel sont basées toutes les communications. Le but de ce modèle est d'être le plus indépendant possible des supports physiques. Pour cela on a défini 4 couches. L'objectif est double :

- Chaque couche est conçue de manière à dialoguer avec son homologue en face, comme si une ***liaison virtuelle*** était établie directement entre elles.

- Chaque couche fournit des services clairement définis à la couche immédiatement supérieure, en s'appuyant sur ceux, plus rudimentaires, de la couche inférieure, lorsque celle-ci existe.

Exemples pour chaque couche :

- Couche Accès Réseau : Ethernet, Technologie (câble, WiFi, Fibre)

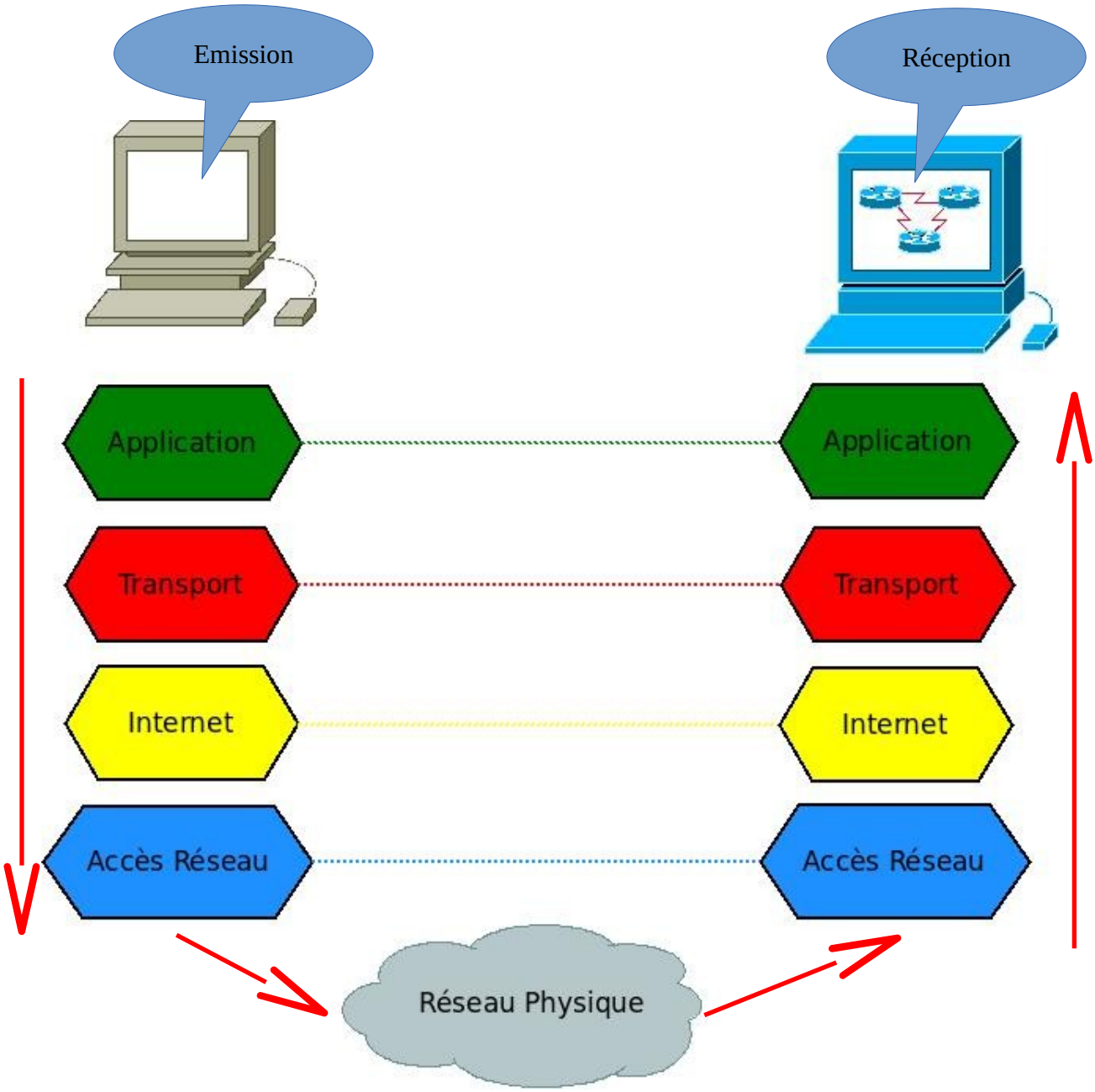
- Couche Internet (Réseau) : @ IP, ARP

- Couche Transport : UDP, TCP

- Couche Application : FTP, HTTP, SMTP, ….

II : Principe de fonctionnement

Lors d'une communication entre deux machines, tout se passe comme si chaque couche était reliée directement avec son homologue en face, c'est ce que l'on appelle une communication de bout en bout.



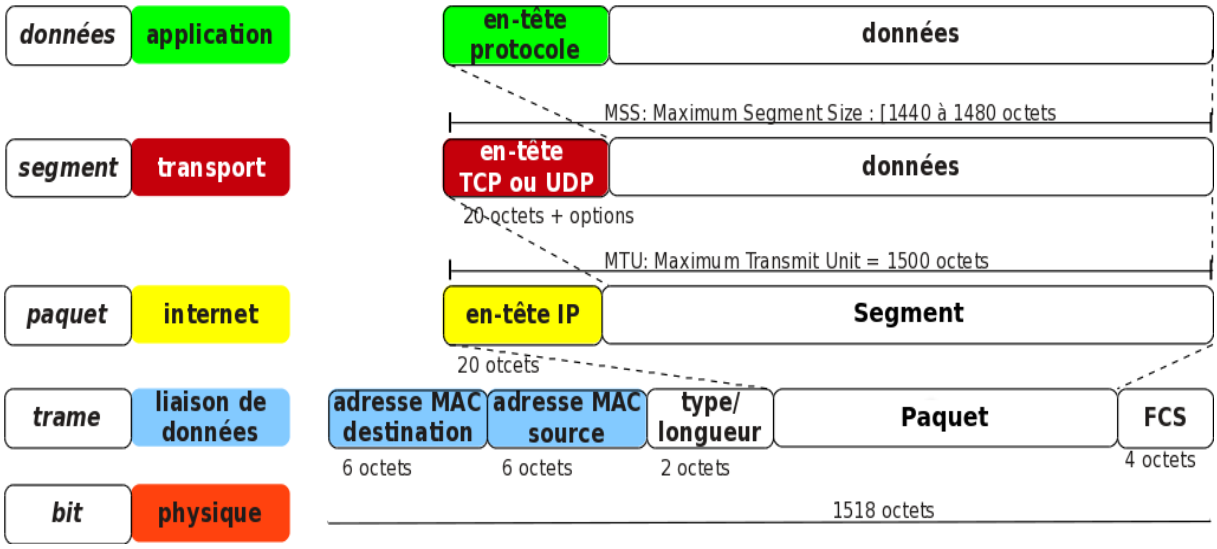
Liaison Virtuelle

Liaison Réelle

III : Principe d'encapsulation des trames

Pour transférer des données, le protocole TCP/IP commence par les découper en 'blocs' de plusieurs centaines d'octets.

Ensuite, chaque couche du modèle TCP/IP va rajouter un entête destiné à son homologue contenant les informations nécessaires au traitement des informations (acheminement, contrôle et ré-assemblage).



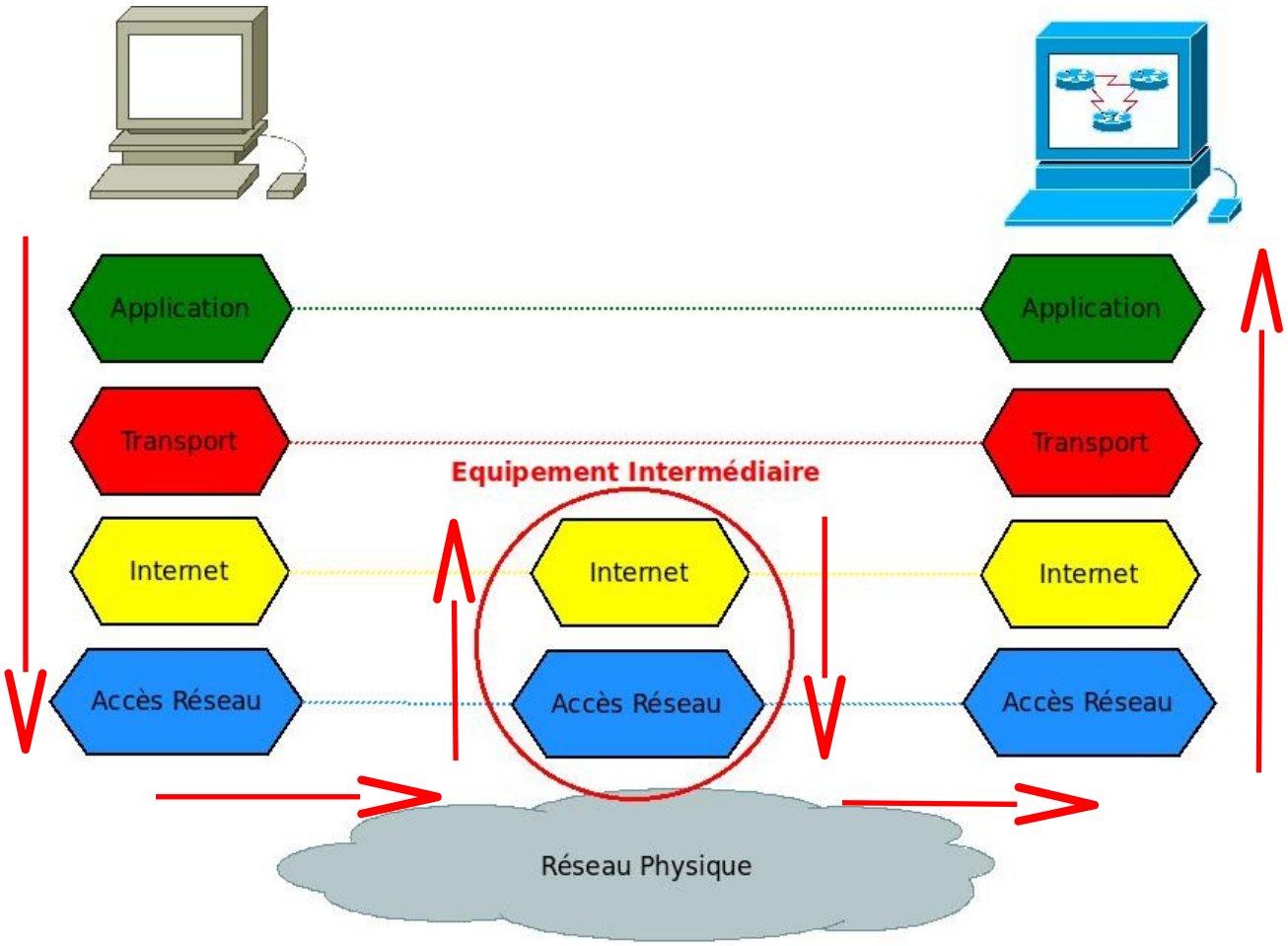
On appelle donnée, les informations issues de la couche application.
On appelle segment, les informations issues de la couche transport (on parle de segment UDP ou segment TCP).
On appelle paquet, les informations issues de la couche internet (on parle de paquet IP).
On appelle trame, les informations issues de la couche accès réseau (on parle de trame Ethernet).

IV : Communication distante

Lors d'une communication entre deux applications distantes (liaison passant par des équipements intermédiaires), les couches Internet et Accès Réseau communiquent avec leur homologue sur l'équipement intermédiaire le plus proche.

Ces équipements modifient alors les entêtes de ces deux couches afin de communiquer avec la prochaine étape, jusqu'à arriver à destination.

Exemple de communication entre deux applications distantes avec un équipement intermédiaire



Liaison Virtuelle

Liaison Réelle

V : La couche Accès Réseau

Son rôle est d'acheminer des données d'une machine X à une machine Y voisine. Les 2 machines sont reliées l'une à l'autre par la même support physique et/ou la même technologie.

Exemple : la technologie Ethernet, support physique WiFi

1) Ethernet (ou standard IEEE 802.3)

Ethernet est un protocole de réseau afin d'échanger des données entre deux machines.

Ethernet utilise la commutation de paquets :

- découpage des données afin d'accélérer le transfert

- chaque trame est composée d'un entête permettant d'aiguiller le paquet sur le réseau vers son point final.

Le protocole Ethernet est indépendant du support physique utilisé, car il est utilisé sur différents supports : Paire Torsadée, Fibre Optique, WiFi...

Il est aussi indépendant de la topologie du réseau utilisée.

On appelle un domaine de diffusion (Broadcast Domain), une zone d'un réseau informatique où n'importe quelle machine peut directement communiquer avec toutes les autres machines du même domaine, dans devoir passer par un routeur.

On appelle un domaine de collision, une zone d'un réseau informatique où les données peuvent entrer en collision entre elles.

2) Câble droit ou croisé ?

On utilise un câble droit pour relier des machines à un commutateur ou un concentrateur. C'est le cas le plus fréquent.

On utilise un câble croisé pour relier directement des machines ou directement des commutateurs ou des concentrateurs (empilage).

Néanmoins de plus en plus de ports (sur les commutateurs ou les machines) sont « Auto-MDX ». Ils croisent ou décroisent automatiquement si le bon câble n'est pas utilisé.

Sur un câble croisé, les fils oranges et verts sont inversés d'une extrémité à l'autre.

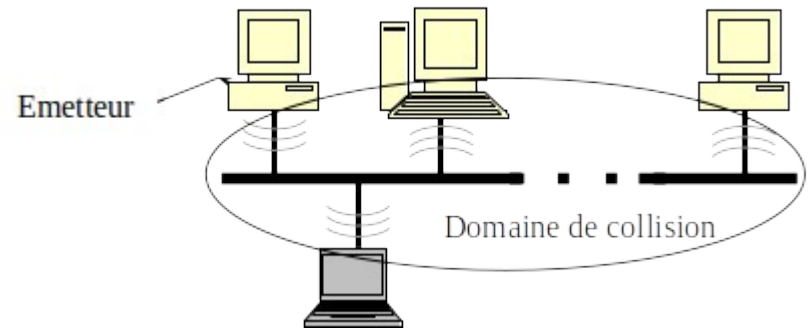
3) Fonctionnement d'un concentrateur (Hub)

Un concentrateur (ou Hub) est un équipement informatique permettant de connecter plusieurs équipements sur un même réseau informatique.

Tous les équipements connectés à un Hub partagent le même domaine de diffusion et le même domaine de collision.

Lorsqu'une donnée arrive sur un concentrateur, celle-ci est renvoyée à tous ses ports, et seul l'équipement concerné la traitera.

Par conséquent, lorsqu'une communication entre deux équipements est en cours, il est impossible d'en avoir une deuxième, car le support physique est occupé.



Remarque : Si deux postes décident d'émettre en même temps, ETHERNET utilise un système de détection de collision (méthode d'accès CSMA/CD). Dans un tel cas, chaque poste attendra un temps aléatoire et refera une tentative.

4) Fonctionnement d'un commutateur (Switch)

Un commutateur (ou Switch) est un équipement informatique permettant de connecter plusieurs équipements sur un même réseau informatique.

Tous les équipements connectés à un Switch partagent le même domaine de diffusion.

Le commutateur peut faire communiquer plusieurs ports en même temps. Pour cela il enregistre dans une table l'adresse MAC des machines branchées sur chacun des ses ports. Il peut ainsi envoyer la trame directement au destinataire.

Lorsqu'une donnée arrive sur un concentrateur, celle-ci est renvoyée uniquement au destinataire, tous les autres ports restent alors disponibles.

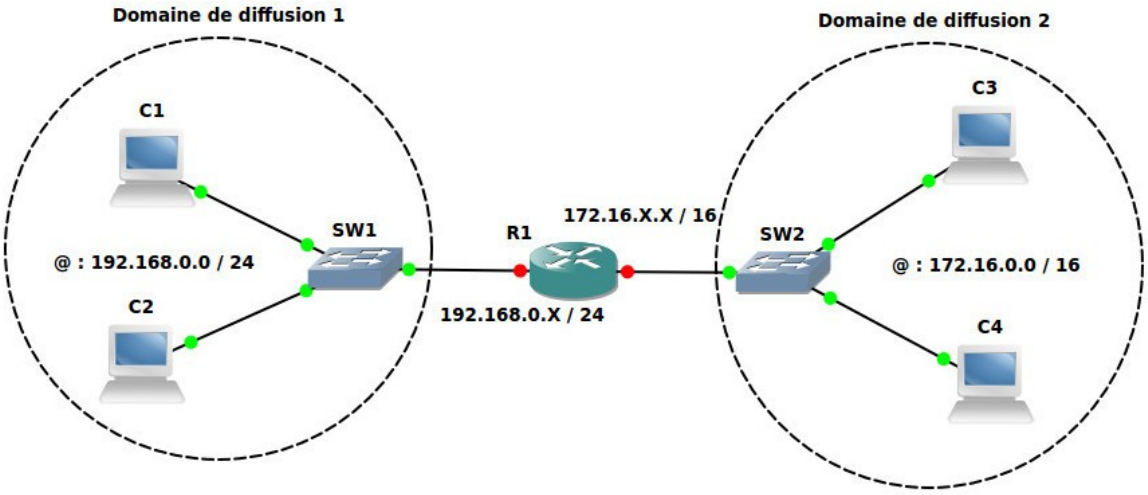
Par conséquent, lorsqu'une communication entre deux équipements est en cours, il est impossible d'en avoir une deuxième avec ces équipements, car le support physique est occupé, mais tous les autres restent disponibles.

5) Principe de fonctionnement d'un routeur

Un routeur est un équipement informatique permettant de relier et de faire communiquer plusieurs domaines de diffusions différents.

Généralement, les machines (ordinateurs, imprimantes,...) ne sont pas directement reliées sur une routeur. Ce sont les concentrateurs et les commutateurs qui sont directement reliés.

Chaque port d'un routeur possède une adresse IP (paramétrable), qui doit être compatible avec les domaines de diffusions qui lui sont connectés.



6) Protocole ARP (Address Résolution protocole)

Bien que tous les équipements d'un réseau informatique possèdent une adresse IP (V4 ou V6), c'est avec les adresses MAC que les communications sont gérées par le protocole Ethernet.

Le protocole ARP permet de ***découvrir l'adresse physique*** (@ MAC) d'un destinataire à partir de son adresse logique (@ IP).

Principe : une machine veut connaître l'@ MAC d'un destinataire :

1- Elle regarde si la réponse ne se trouve pas dans sa table d'adresses physiques (qui est enregistrée en local sur la machine)

2- Elle envoie une requête ARP ***avec l'@IP à traduire*** à tout le domaine de diffusion en broadcast : @MAC= FF:FF:FF:FF:FF:FF

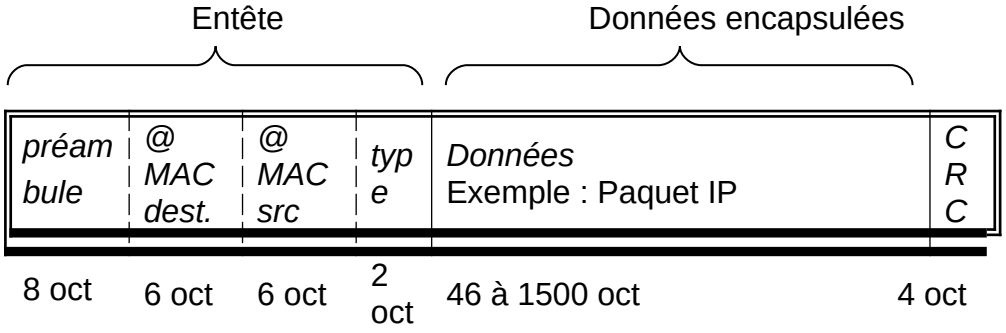
3- La machine à qui appartient ***l'@ IP à traduire*** renvoie son @ MAC à la machine qui à fait la demande. Si l'@MAC n'est pas présente sur le domaine de diffusion, c'est l'adresse de la passerelle qui sera donnée.

4- La machine qui a fait la demande enregistre temporairement la réponse dans sa table

7) Trame Ethernet

Ethernet, comme toutes les couches du modèle TCP/IP ajoute son entête afin de gérer les communication de proche en proche.

Trame Ethernet II :



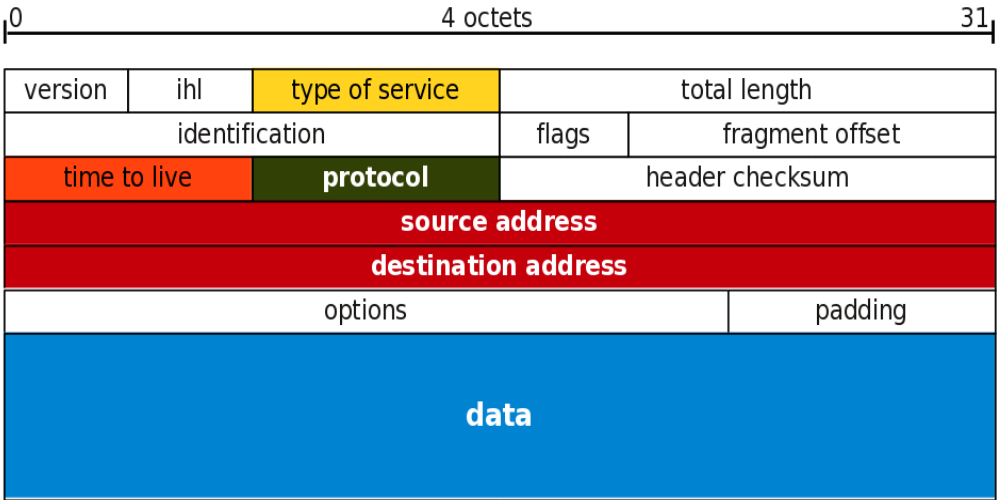
- *Préambule* : Horloge de synchronisation avec les récepteurs
- *@ MAC dest*. : Adresse MAC du destinataire
- *@ MAC src* : Adresse MAC de l'émetteur de la trame
- *type* : Code identifiant le protocole de niveau supérieur contenu dans le champ « *Données* ». Principaux types : 0800 : IPV4 ; 86DD : IPV6 ; 0806 : ARP ; 8035 : RARP
- *Données* : C'est ici que la trame de niveau supérieur est encapsulée
- *CRC* : (Cyclic Redundancy Check) mécanisme de détection d'erreur

VI : Couche Internet

Le principe principal du protocole TCP/IP est de permettre une communication en mode non connecté (c'est à dire sans avoir besoin d'une liaison directe entre les deux machines). Les données sont découpées en paquet et chaque paquet est indépendant et peut suivre un itinéraire différent jusqu'à la destination.

La couche internet ne propose aucun contrôle de communication (perte de paquet, ordre, …). C'est la couche transport qui gère cette fonction.

Détail de l'entête IP :



- Version (4 bits) : Version d'@IP utilisé.

- IHL (Internet Header Lenghts – 4 bits) : taille de l'entête IP en nombre de groupes de 4 octets.

- Type Of Service (TOS – 1 octet) : Type de service, permet de prioriser les paquets IP

- Total Lenght (2 octets) : longueur totale en octets du paquets IP, entête comprise.

- Identification (2 octets) : Utilisé pour numéroter les paquets en cas de découpage ultérieur (on parle alors de fragment).

- Flags (3 bits) : Informations sur la fragmentation.

- Fragment Offset (13 bits) : numéro de fragment en cas de découpage par rapport au premier en nombre de mots de 8 octets

- Time To Live (TTL – 1 octet) : durée de vie du paquet IP en nombre d'étapes (routeurs). Si = 0, le paquet est détruit.

- Protocol (1 octet) : protocole utilisé par la couche transport ; TCP = 6 ; UDP = 17 ; ICMP = 1

- Header Checksum (2 octets) : Contrôle de la validité de l'entête

- Source Address (4 octets) : @ IP de la machine source

- Destination Address (4 octets) : @ IP de la machine de destination

- Options (de 0 à 40 octets) : facultatif

- Padding (taille variable) : remplissage pour arriver à un nombre d'octet multiple de 4.

VII : Couche transport

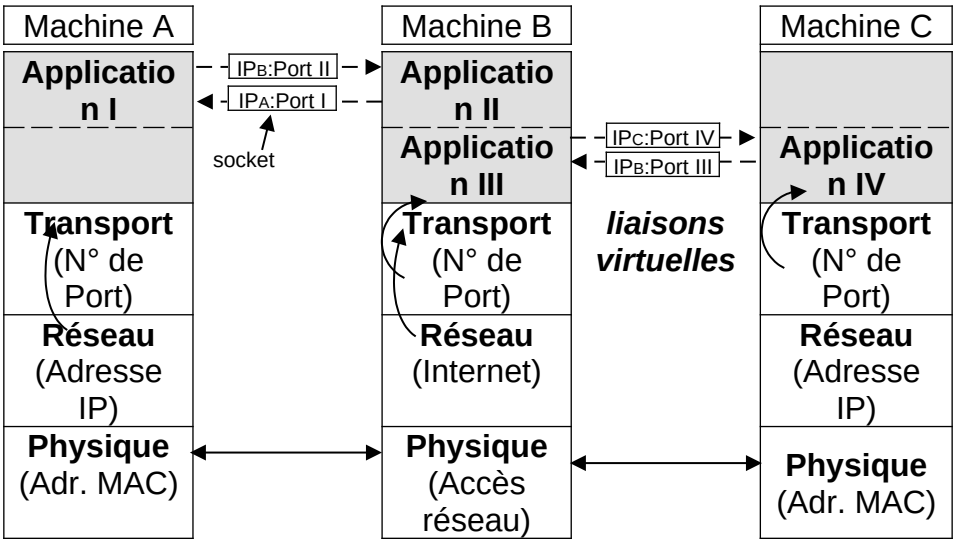
Rôle de la couche transport :

- Acheminer la donnée à la bonne application de la machine

- Segmenter la donnée en trames sur la machine source, la reconstituer à destination en assurant le contrôle de l'acheminement (TCP uniquement).

1) Notion de port

Une adresse IP correspond à une machine (cliente ou serveur). Par contre une machine peut avoir plusieurs applications qui envoient ou reçoivent des données. Pour qu'une application I sur une machine A puissent communiquer avec une application II sur une machine B il faut qu'elles puissent se retrouver sur chaque machine : Le **port**.



Quelques ports par défaut sur les serveurs :

- 21 : FTP
- 23 : TELNET
- 25 : SMTP
- 53 : DNS
- 80 : HTTP
- 110 : POP3
- 443 : HTTPS
- 5060 : SIP

Le client qui établi une communication ouvre un port à partir de 1024. S'il établi une autre communication (simultanément ou après) il ouvrira le port suivant (1025) etc…

2) Protocole UDP (RFC768)

Entête UDP **Données Encapsulées**

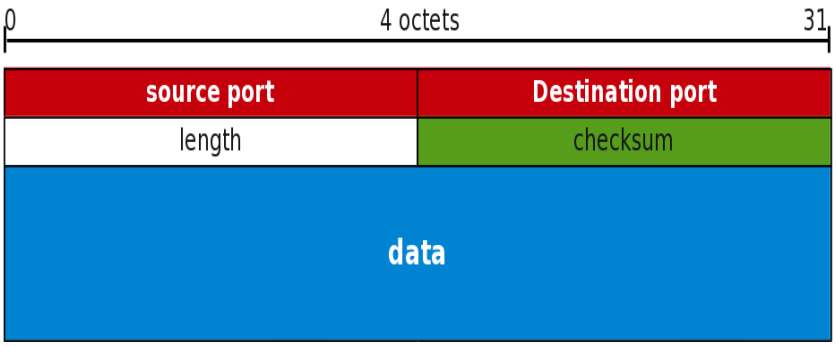
Port SRC.	*Port DEST.*	*Long*	*Check-sum.*	*Données* Exemple : Partie de page HTML

- Le segment UDP est encapsulé dans un paquet IP.

- Le protocole UDP est très simple mais il ne fournit aucun contrôle.

- Son seul rôle est de d'acheminer la donnée à la bonne applications en fonction du n° de ports (Multiplexage/Démultiplexage)

Détail de l'entête UDP



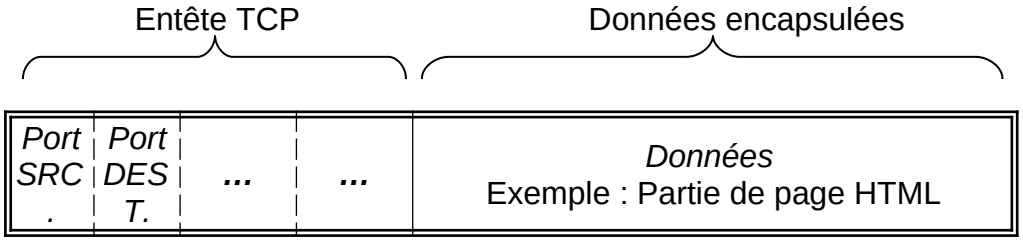
- Source Port (2 octets) : Indique par quel port le paquet a été envoyé

- Destination port (2 octets) : Indique sur quel port le paquet est envoyé

- Lenght (2 octets) : Longueur totale du segment UDP (entête compris) en octets.

- Checksum (2 octets) : Contrôle de validité du paquet.

3) Protocole TCP (RFC793)



Le segment TCP est encapsulé dans un paquet IP.

Le rôle de TCP est multiple :

- Contrôler l'acheminement des paquets IP

La couche IP (Routage) étant sans garantie, TCP établi une connexion entre client et serveur (**SYN** + **ACK**) puis contrôle que tous les segments ont bien été transférés (**N° d'ordre** + **N° d'accusé de réception** + **ACK**). Au besoin il fait ré acheminer les segments manquants.

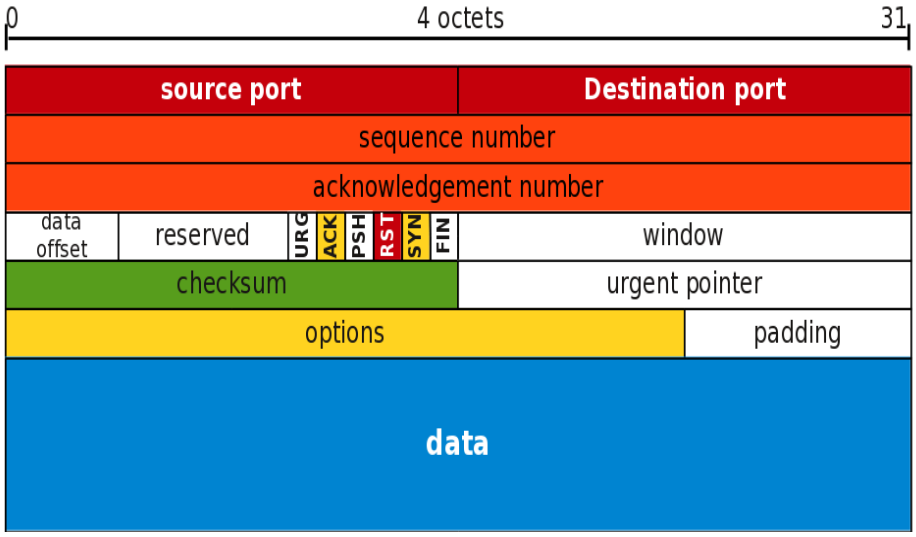
- Multiplexer/Démultiplexer le transfert de données

TCP permet à une machine de connecter plusieurs applications en même temps en utilisant (« ouvrant ») plusieurs ports.

- Réguler le débit des données en transférant des segments de tailles variables.

- Éventuellement établir des priorités et sécuriser la communication.

Détail de l’entête TCP



- Source Port (2 octets) : Indique par quel port le paquet a été envoyé

- Destination port (2 octets) : Indique sur quel port le paquet est envoyé

- Sequence Number (4 octets) : numéro de séquence du premier octet de ce segment.

- Acknowledgement Number (4 octets) : numéro de séquence du prochain octet attendu.

- Data Offset (4 bits) : Taille de l'entête TCP en nombre de groupes de 4 octets.

- Divers Drapeaux (12 bits) : informations de contrôle

- Window (2 octets) : Taille de fenêtre demandée, c'est à dire nombre d'octets que le receveur souhaite recevoir sans accusé de réception.

- Checksum (2 octets) : Contrôle de validité du paquet.

- Urgent Pointer (2 octets) : Pointeur de données urgentes.

- Options (X octets) : facultatif

- Padding (taille variable) : remplissage pour arriver à un nombre d'octet multiple de 4.

VIII : Principaux services sur un réseau informatique

Ces principaux services se trouvent dans quasiment tous les réseaux informatiques. Généralement, ces services sont configurés automatiquement (ce qui a permis d'apporter Internet chez M. “tout le monde”).

Il est toutefois possible de les configurer manuellement (permet des réglages plus fins), mais il faut bien sûr savoir à quoi correspondent ces différents services.

1) DNS (Domaine Name Server)

Un serveur DNS est une machine capable de découvrir l’adresse IP d’une destination à partir de son nom de domaine.

Ex : www.ac-grenoble.fr = 193.54.149.12

Les serveurs DNS sont généralement situés sur Internet et mis à disposition par le fournisseur d’accès à Internet (FAI ou Provider)

Avant toute requête sur l’Internet avec un nom de domaine, il y a avant une requête DNS.

Sans nom de domaine, l’Internet serait quasi impossible.

2) Notion de Passerelle (Gateway)

Lorsqu'une machine n'est pas présente sur le domaine de diffusion, il faut passer par un routeur.

La passerelle correspond à l'adresse du port du routeur par lequel doivent passer les informations pour accéder à d'autres domaines de diffusions.

3) DHCP

Le service DHCP permet de distribuer automatiquement des adresses IP aux machines d’un sous réseau.

Sur le serveur DHCP il faut définir impérativement :

- une plage d’adresse. Ex : 192.168.0.100 à 192.168.0.200
- un masque de sous réseau
- un bail (durée de validité de l'adresse). Ex : 1 jour

En option on peut aussi définir :

- l’adresse de la passerelle par défaut des clients

- l’adresse du (des) serveur(s) DNS des clients

- Exclure certaines adresses de la plage

- Réserver un adresse IP à une machine en particulier grâce à l’adresse mac

Attention : le serveur DHCP doit avoir une adresse IP compatible avec le sous réseau (Ex : 192.168.0.2). Pour pouvoir distribuer des adresses IP dans un autre sous réseau, il faut mettre un service « Agent de relais DHCP » dans l’autre sous réseau.

Sous Windows en « Invite de commandes », 3 commandes sont utiles quand on utilise le service DHCP :
- "ipconfig / renew" pour demander ou renouveler une adresse IP sans attendre
- "ipconfig / release" pour abandonner une adresse IP
- "ipconfig / all" pour voir tous les détails de l’adresse obtenue

4) Proxy

Dans un réseau où il y a un serveur Proxy, les machines ne peuvent pas aller directement sur Internet chercher des pages Web.

Pour obtenir une page, le client effectue une demande au proxy qui répondra positivement ou non (en fonction de sa configuration)

La passerelle Internet doit être configurée pour bloquer les requêtes des clients et n’autoriser que le serveur Proxy.

Fréquemment le Proxy est intégré à la passerelle Internet.

5) Pare feu

Le pare-feu analyse chaque trame qu’il reçoit. Il la compare à toutes les règles de filtrage qui ont été définies par l’administrateur une à une jusqu’à trouver une règle qui corresponde. En fonction de la règle, la trame est transmise ou éliminée.

En générale, la dernière règle élimine d’office la trame. Autrement dit, « tout ce qui n’est pas autorisé est interdit »