Réseaux

Organisation de l'UE

- Cours : 12h
- TD : 12h
- TP : 14h (dont une partie projet)
  - Cours et TD : Djamal Habet
  - TP : Emmanuel Godard
- Supports : disponibles sur AMETICE

Evaluation de l'UE

- Session 1 : $\frac{2}{3}ET + \frac{1}{3}TP$
- Session 2 : $Max(ET, \frac{2}{3}ET + \frac{1}{3}TP)$
  - ET : Examen Terminal
  - TP : Note de TP (dont Projet)

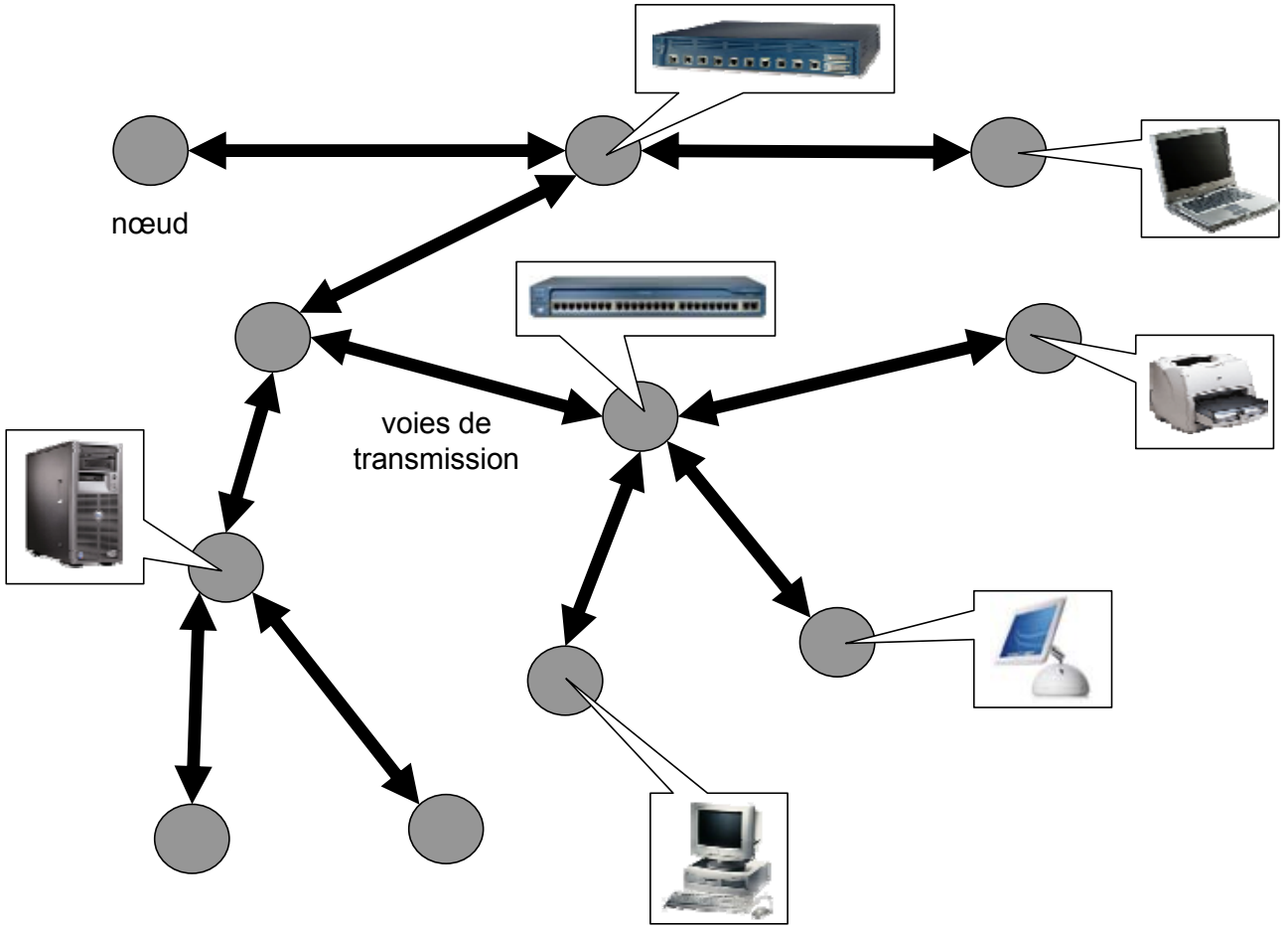
Contenu de l'UE

- Introduction et notions de base
- Modèle OSI
- Pile TCP/IP
- Applications

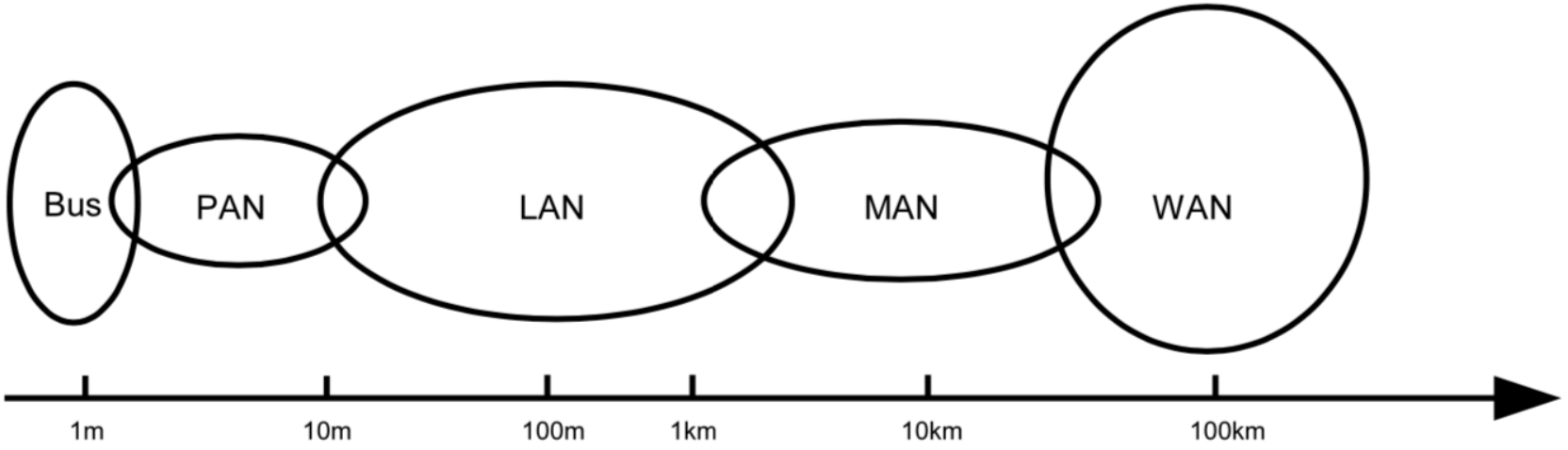
Introduction

- Les réseaux informatiques permettaient à leur origine de relier des terminaux passifs à de gros ordinateurs centraux
- Actuellement : interconnexion de plusieurs types de matériel,
  - Gros serveurs, stations de travail, ordinateurs personnels, tablettes, smartphones, etc.
- Les services offerts font partie de la vie courante :
  - Entreprises et administrations (banques, gestion, commerce, recherche, etc.)
  - Particuliers (messagerie, loisirs, services informatiques par Internet, etc.).

Réseau Informatique



Taille des réseaux



Taille des réseaux

- Bus : dans un ordinateur pour relier ses différentes composantes (mémoires, périphériques d'entrée-sortie, processeurs, etc.) peuvent être considérés comme des réseaux dédiés à des tâches très spécifiques.

- Réseau personnel (Personnal Area Network) : interconnecte (souvent par des liaisons sans fil) des équipements personnels comme un ordinateur portable, un smartphone, une imprimante, etc. Un cluster est un groupe d'unités centrales reliées entre elles de manière à agir comme un seul ordinateur soit pour pouvoir faire de la répartition de charges soit du calcul distribué.

Taille des réseaux

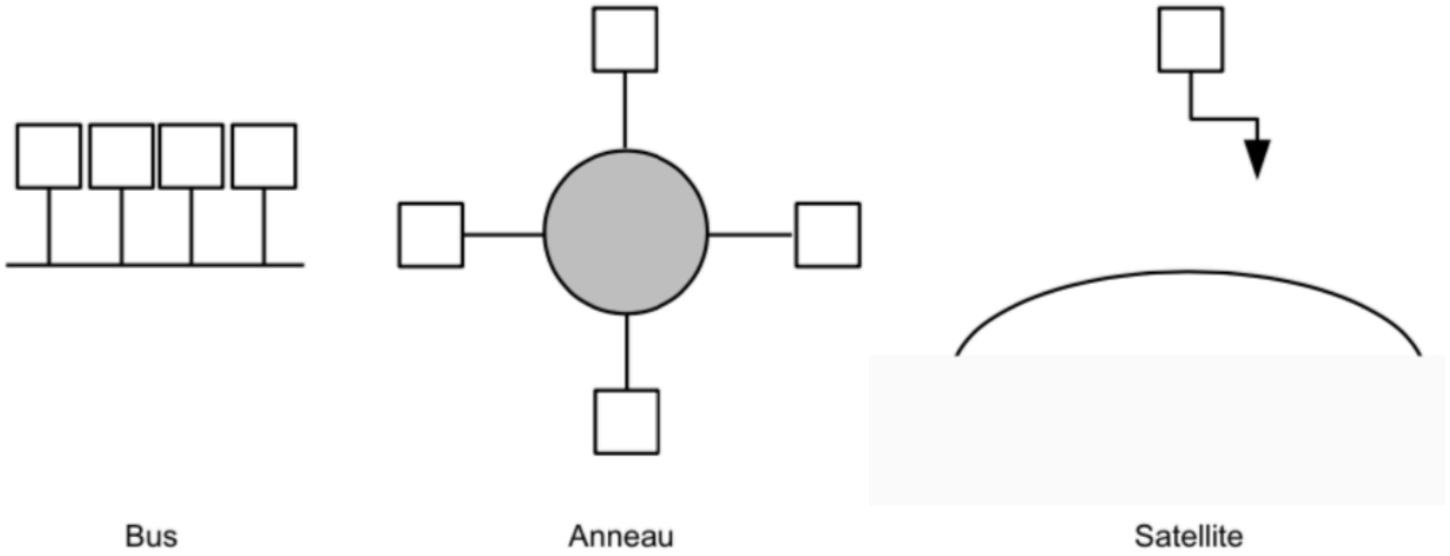
- Réseau local (Local Network) : peut s'étendre de quelques mètres à quelques kilomètres et correspond au réseau d'une entreprise. Il peut se développer sur plusieurs bâtiments et permet de satisfaire tous les besoins internes de cette entreprise.

- Réseau métropolitain (Metropolitan Area Network) : interconnecte plusieurs lieux situés dans une même ville, par exemple les différents sites d'une université ou d'une administration, chacun possédant son propre réseau local.

- Réseau étendu (Wide Area Network) : permet de communiquer à l'échelle d'un pays, ou de la planète entière, les infrastructures physiques pouvant être terrestres ou spatiales à l'aide de satellites de télécommunication.

Topologie des réseaux

Mode en diffusion



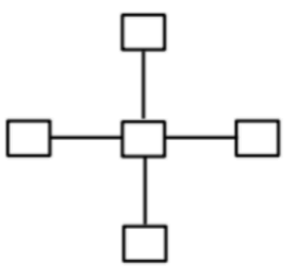
Topologie des réseaux

Mode en diffusion :

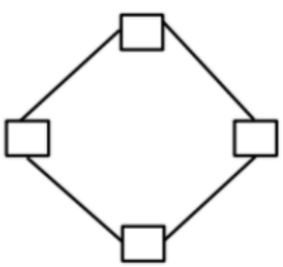
- consiste à partager un seul support de transmission.
- Chaque message envoyé par un équipement sur le réseau est reçu par tous les autres.
- C'est l'adresse spécifique placée dans le message qui permettra à chaque équipement de déterminer si le message lui est adressé ou non.
- A tout moment, un seul équipement a le droit d'envoyer un message sur le support
- Il faut donc qu'il "écoute" au préalable si la voie est libre; si ce n'est pas le cas il attend selon un protocole spécifique à chaque architecture.
- Les réseaux locaux adoptent pour la plupart le mode diffusion sur une architecture en bus ou en anneau
- La rupture du support provoque l'arrêt du réseau, par contre la panne d'un des éléments ne provoque pas (en général) la panne globale du réseau

Topologie des réseaux

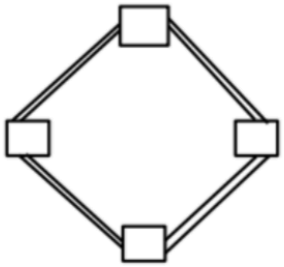
Mode point à point



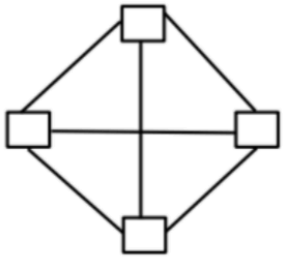
Étoile



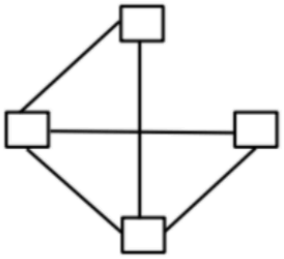
Boucle simple



Boucle double



Maillage régulier



Maillage irrégulier

Topologie des réseaux

Mode point à point :

- Le support physique (le câble) relie une paire d'équipements seulement.
- Quand deux éléments sont directement connectés entre eux veulent communiquer ils le font par l'intermédiaire des autres noeuds du réseau.
- L'étoile : le site central reçoit et envoie tous les messages, le fonctionnement est simple, mais la panne du noeud central paralyse tout le réseau.
- Boucle simple : chaque noeud recevant un message de son voisin en amont le réexpédie à son voisin en aval. Pour que les messages ne tournent pas indéfiniment, le noeud émetteur retire le message lorsqu'il lui revient. Si l'un des éléments du réseau tombe en panne, alors tout s'arrête.
- Double boucle : chacune des boucles fait tourner le message dans le sens opposé. En cas de panne d'un équipement, on reconstitue une boucle simple avec les éléments actifs des deux boucles, mais dans ce cas tout message passera deux fois par chaque noeud. Il en résulte alors une gestion très complexe.
- Maillage régulier : l'interconnexion est totale ce qui assure une fiabilité optimale du réseau, par contre c'est une solution coûteuse en câblage physique.
- Si l'on allège le plan de câblage, le maillage devient irrégulier et la fiabilité peut rester élevée mais elle nécessite un acheminement des message selon des algorithmes parfois complexes. Dans cette architecture, il devient presque impossible de prévoir le temps de transfert d'un noeud à un autre.

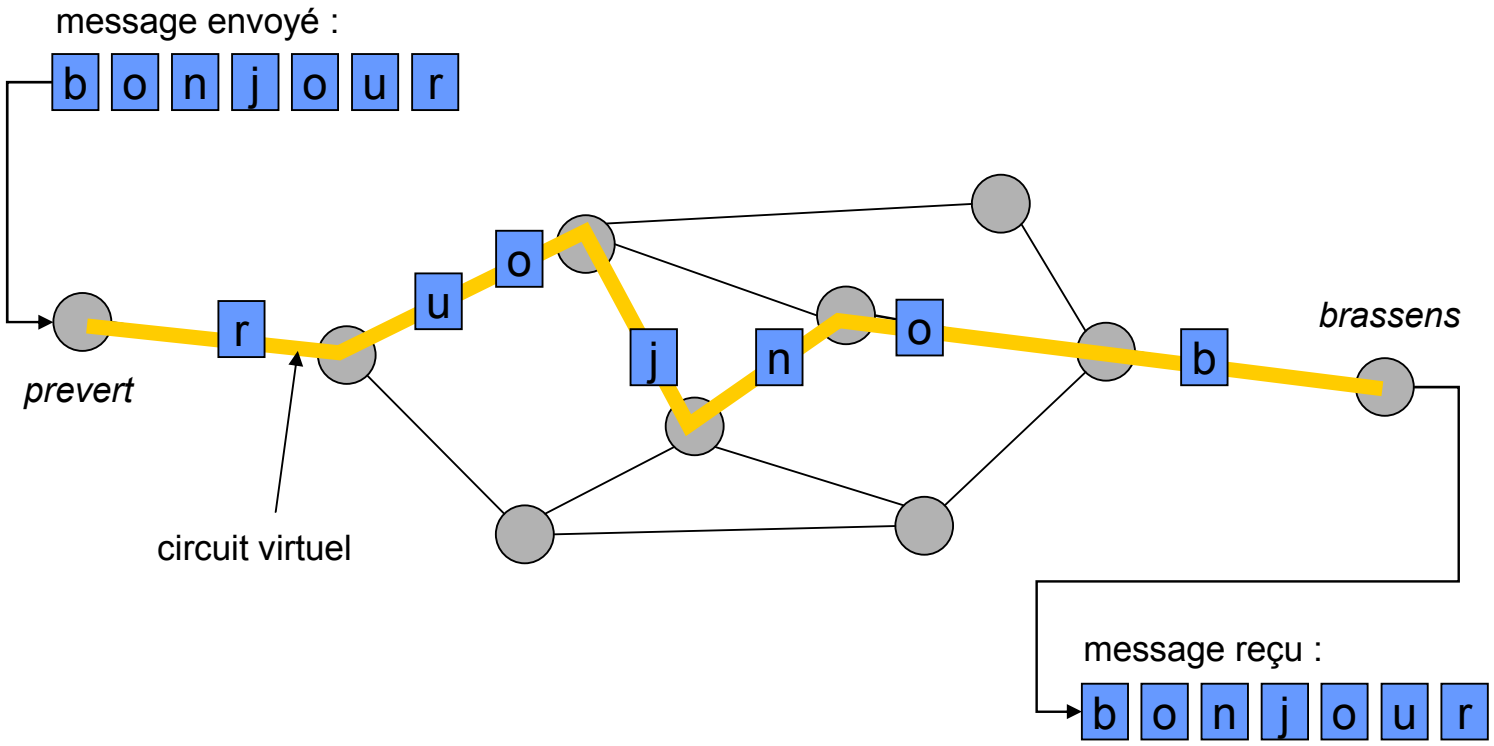
Communication dans les réseaux

- Communication avec connexion :

1. l'émetteur demande l'établissement d'une connexion par l'envoi d'un bloc de données spécial,
2. si le récepteur (ou le gestionnaire de service) refuse cette connexion, alors la communication n'aura pas lieu,
3. si la connexion est acceptée, elle est établie par la mise en place d'un circuit virtuel dans le réseau reliant l'émetteur au récepteur,
4. les données sont ensuite transférées d'un point à l'autre,
5. la connexion est libérée.

Communication dans les réseaux

- Communication avec connexion :



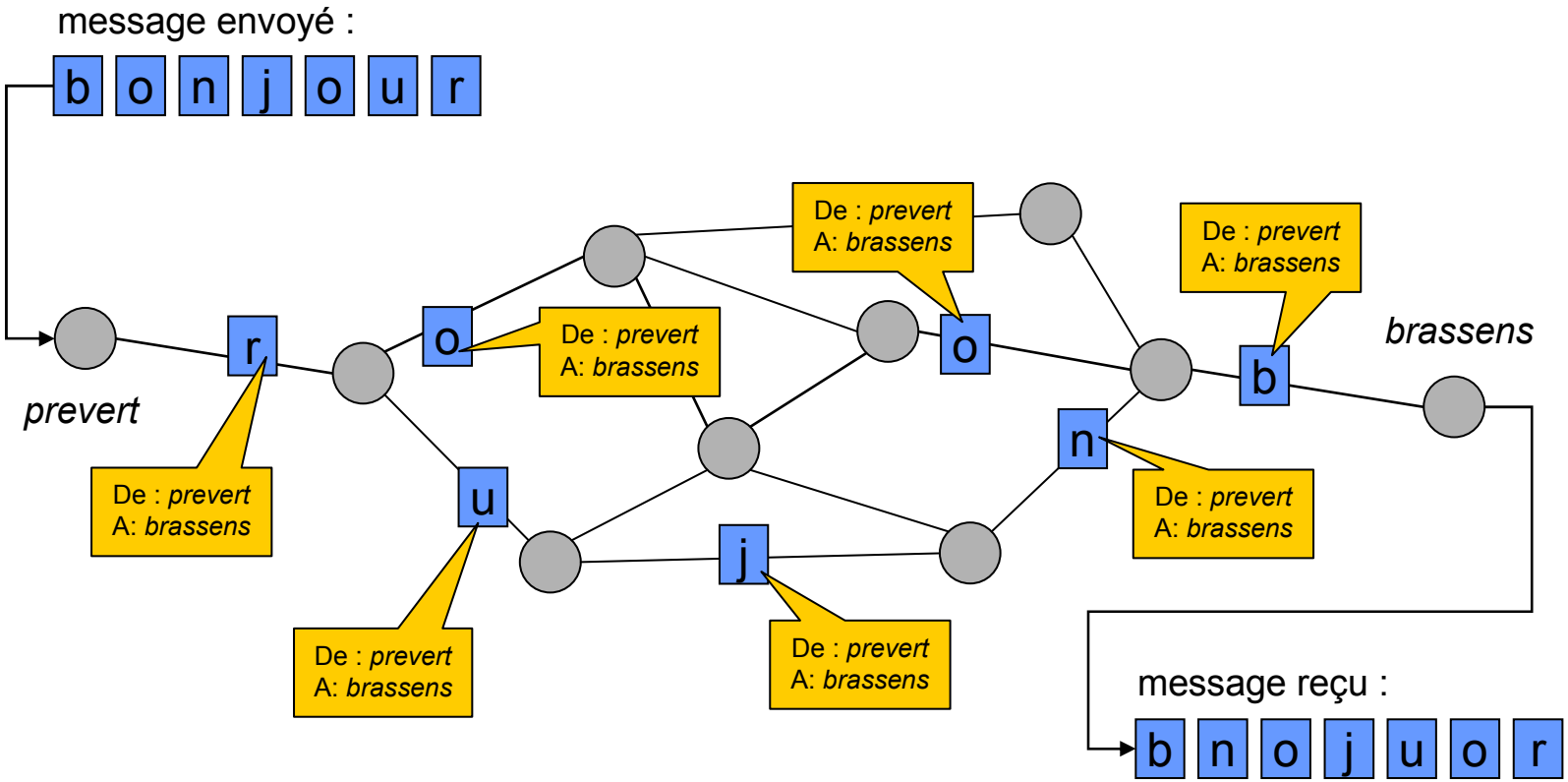
Communication dans les réseaux

- Communication sans connexion : les blocs de données, appelées *datagrammes*, sont émis sans vérifier à l'avance si l'équipement à atteindre, ainsi que les noeuds intermédiaires éventuels, sont bien actifs.

  1. le client poste une lettre dans une boîte aux lettres,
  2. chaque lettre porte un nom et l'adresse du destinataire,
  3. chaque client a une adresse propre et une boîte aux lettres,
  4. le contenu de l'information reste inconnu du prestataire de service,
  5. les supports de transport sont inconnus de l'utilisateur de service.

Communication dans les réseaux

- Communication sans connexion :



Commutation dans les réseaux

- Commutation de circuits :
  - Historiquement la première à être utilisée, par exemple dans le réseau téléphonique à l'aide des auto-commutateurs.
  - Elle consiste à créer dans le réseau un circuit entre l'émetteur et le récepteur avant que ceux-ci commencent à échanger des informations.
  - Ce circuit sera propre aux deux entités communiquant et il sera libéré lorsque l'un des deux coupera sa communication.
  - Par contre, si pendant un certain temps les deux entités ne s'échangent rien le circuit leur reste quand même attribué.
  - Un même circuit (ou portion e circuit) pourra être attribué à plusieurs communications en même temps. Cela améliore le fonctionnement global du réseau mais pose des problèmes de gestion (files d'attente, mémorisation, etc.).

Commutation dans les réseaux

- Commutation de messages :
  - Elle consiste à envoyer un message de l'émetteur jusqu'au récepteur en passant de noeud de commutation en noeud de commutation.
  - Chaque noeud attend d'avoir reçu complètement le message avant de le réexpédier au noeud suivant.
  - Cette technique nécessite de prévoir de grandes zones tampon dans chaque noeud du réseau, mais comme ces zones ne sont pas illimitées il faut aussi prévoir un contrôle de flux des messages pour éviter la saturation du réseau.
  - Il devient très difficile de transmettre de longs messages (taux d'erreurs de transmission élevé)

Commutation dans les réseaux

- Commutation de paquets :
  - Un message émis est découpé en paquets et par la suite chaque paquet est commuté à travers le réseau comme dans le cas des messages.
  - Les paquets sont envoyés indépendamment les uns des autres et sur une même liaison on pourra trouver les uns derrière les autres des paquets appartenant à différents messages.
  - Chaque noeud redirige chaque paquet vers la bonne liaison grâce à une table de routage.
  - La reprise sur erreur est plus simple que dans la commutation de messages
  - Le récepteur final doit être capable de reconstituer le message émis en réassemblant les paquets.
    - Nécessite un protocole particulier car les paquets peuvent ne pas arriver dans l'ordre initial, soit parce qu'ils ont empruntés des routes différentes, soit parce que l'un d'eux a du être réémis suite à une erreur de transmission.

Commutation dans les réseaux

- Commutation des cellules :
  - Une cellule est un paquet particulier dont la taille est toujours fixée 53 octets (5 octets d'en-tête et 48 octets de données).
  - Technique de base des réseaux hauts débits ATM (Asynchronous Transfert Mode) qui opèrent en mode connecté
  - Cette technique mixe la commutation de circuits et la commutation de paquets de taille fixe permettant ainsi de simplifier le travail des commutateurs pour atteindre des débits plus élevés.

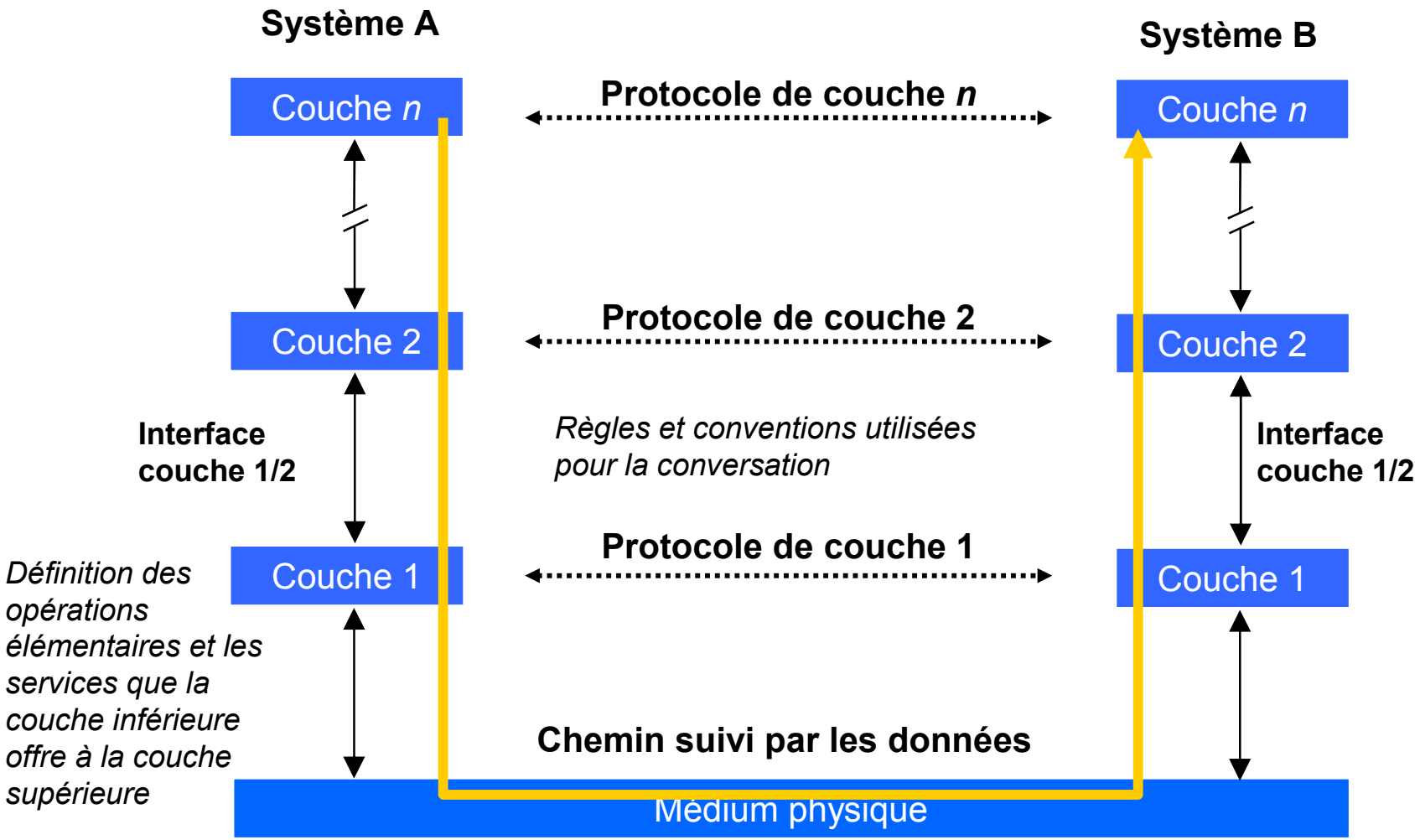
La normalisation

- Distinction norme / standard
  - La norme est établie par un organisme dont c'est officiellement le rôle
  - Le standard, ou standard de fait (*defacto standard*) est comparable mais rédigé par une entité non reconnue et avec des engagements de pérennité plus limités
- Rôle des organismes de normalisation
  - Définir un cadre de développement et d'évolution des technologies, souvent nommé modèle
  - Garantir la complétude et l'intégrité des spécifications
- Organismes les plus connus :
  - ISO : International Standard Organisation
  - ITU (ex CCITT) : International Telecommunication Union
  - IEEE : Institute of Electrical and Electronic Engineers

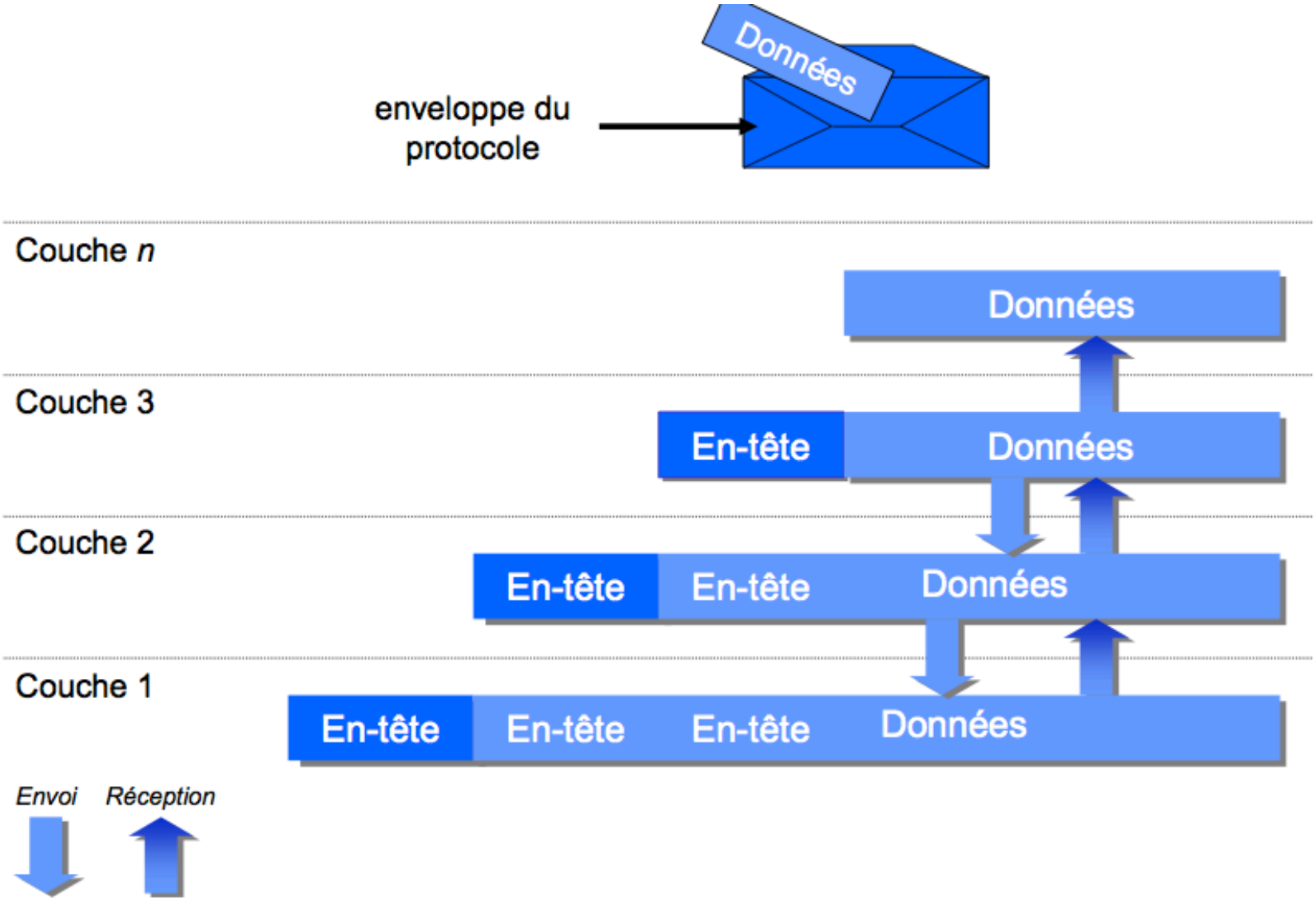
Le modèle OSI
Operated Open System

- Années 70 : ISO démarre une réflexion sur une architecture de réseau en couches
  - Un double objectif pour permettre à l'utilisateur :
    - de modifier dans le temps son infrastructure en ne remplaçant que le ou les modules (matériels ou logiciels) nécessaires
    - de se procurer les modules constitutifs de son architecture chez différents fournisseurs
- Définition du modèle OSI
  - Open : systèmes ouverts à la communication avec d'autres systèmes
  - Systems : ensemble des moyens informatiques (matériel et logiciel) contribuant au traitement et au transfert de l'information
  - Interconnection

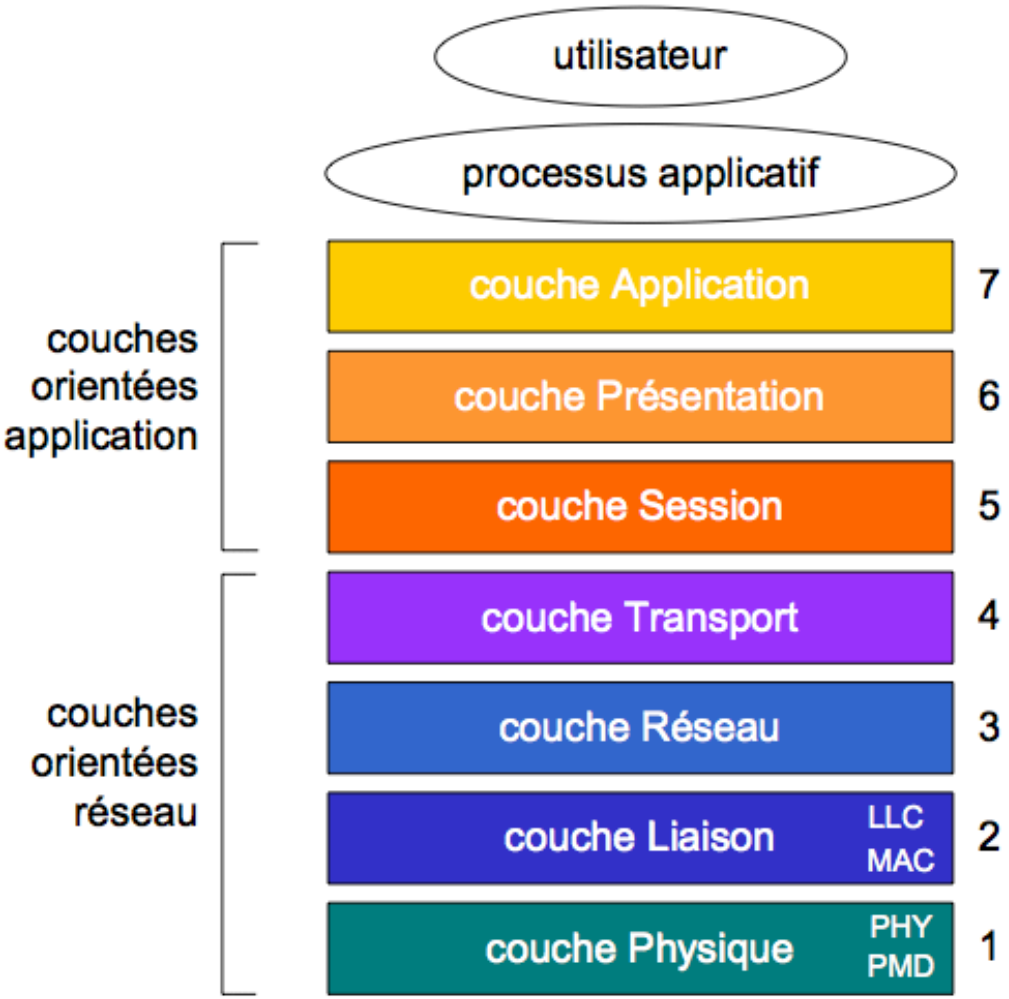
Le modèle OSI



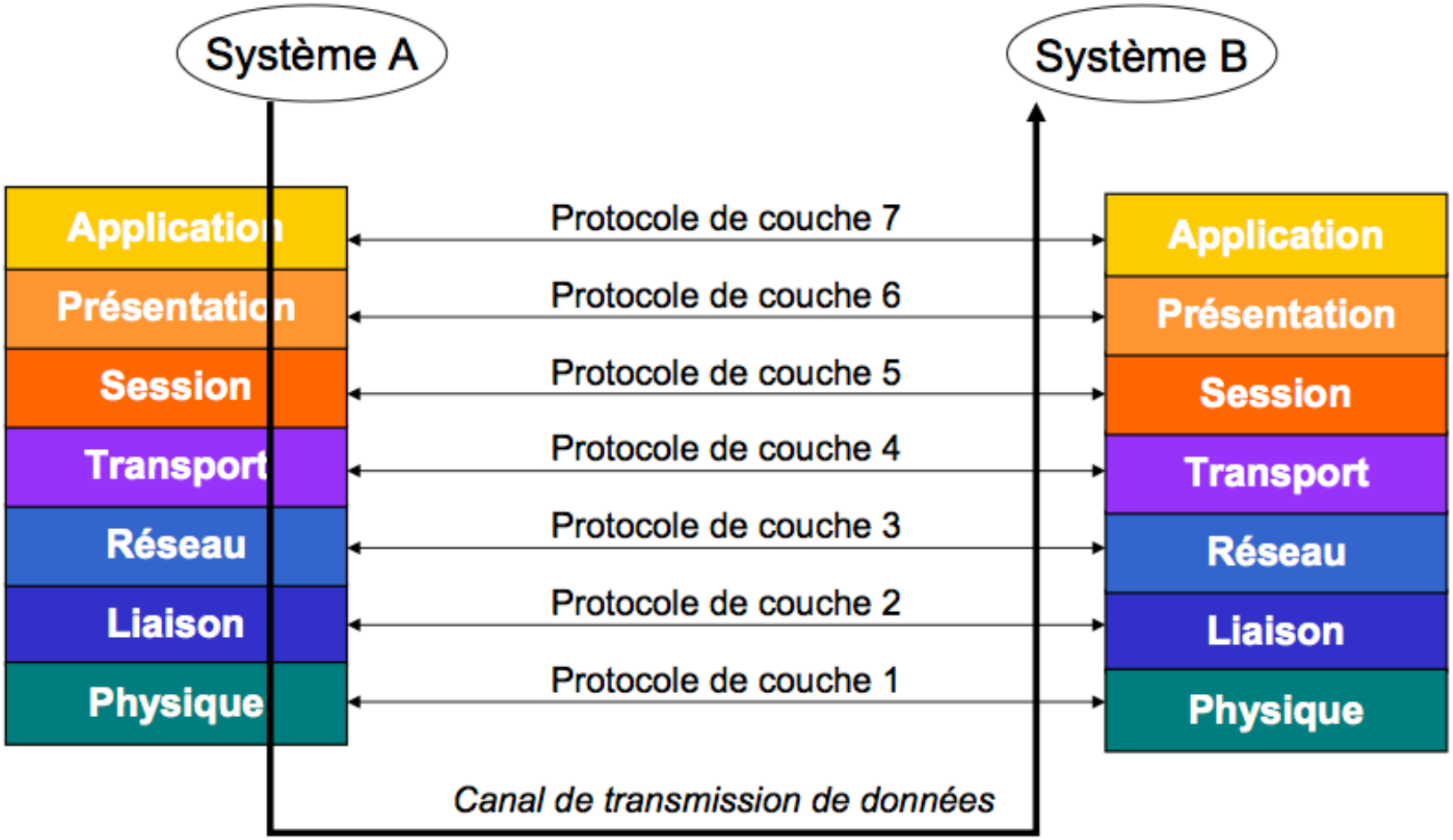
Encapsulation des données



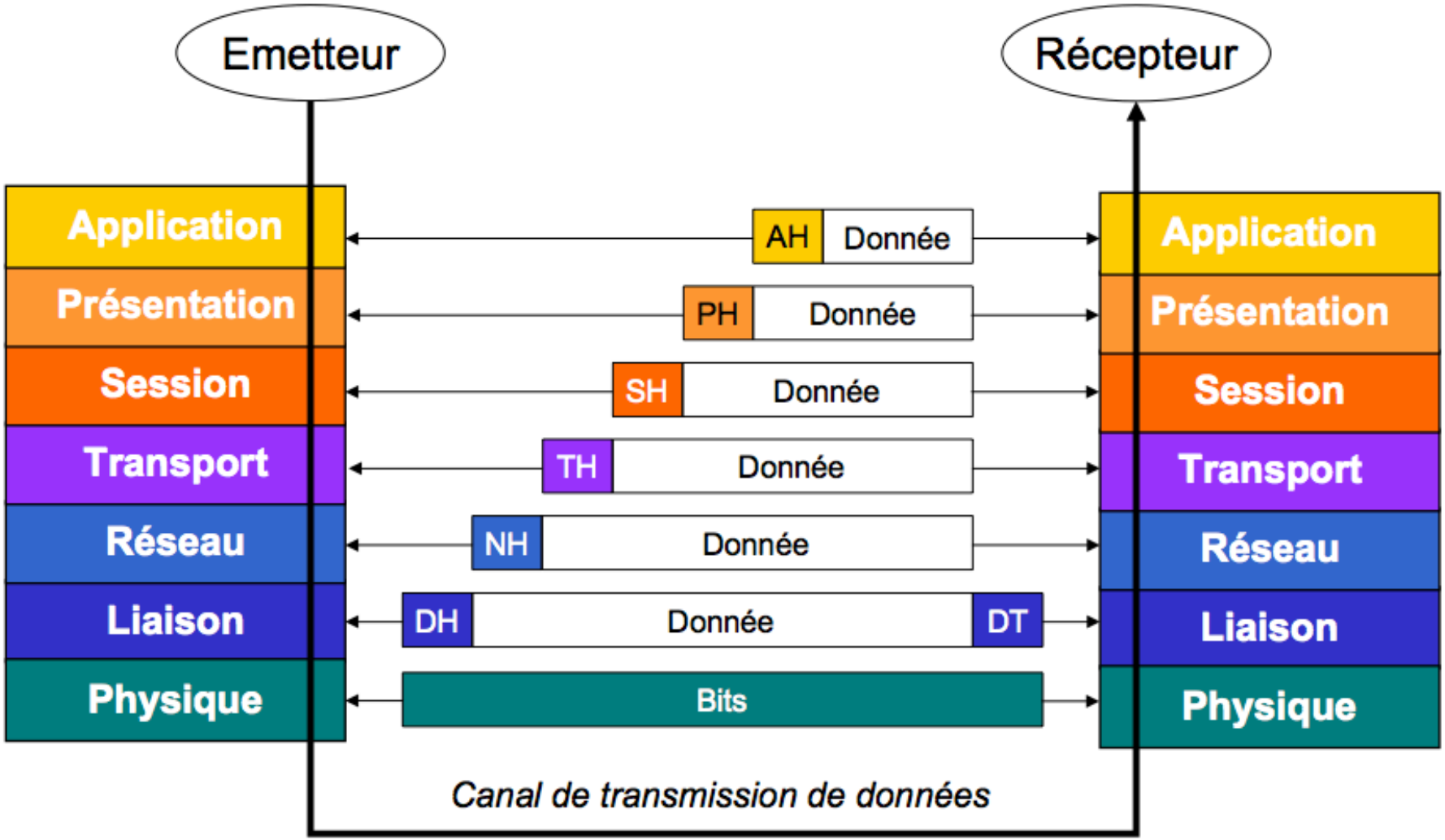
Le modèle OSI



Le modèle OSI



Le modèle OSI



Le modèle OSI

- AH : Entête d'application (Application Header)
- PH : Entête de présentation (Presentation Header)
- SH : Entête de session (Session Header)
- TH : Entête de transport (Transport Header)
- NH : Entête de réseau (Network Header)
- DH : Entête de liaison de données (Data Header)
- DT : Délimiteur de fin de trame (Data Trailer)

Couche physique

- La couche physique fournit les moyens mécaniques, électriques, fonctionnels et procéduraux nécessaires à l'activation des connexions physiques destinées à la transmission de bits entre deux entités de liaison de données.
- On s'occupe de la transmission des bits de façon brute
  - le type des signaux émis (modulation, puissance, portée, .etc.)
  - la nature et les caractéristiques des supports (câble, fibre optique, etc.)
  - les sens de transmission, etc.
- Un bit envoyé à 1 par la source doit être reçu comme un bit à 1 par la destination

Sens de transmission

- Plusieurs possibilités de sens de transmission
  - mode simplex : transmission unidirectionnelle, de l'émetteur vers le récepteur
  - mode semi-duplex (half duplex) ou bidirectionnel à l'alternat : transmission dans les 2 sens possibles mais alternativement.
  - mode duplex (full duplex) ou bidirectionnel simultané : transmission simultanée dans les deux sens

Transmission parallèle

- Les bits d'un même caractère sont envoyés en même temps chacun sur un fil distinct
- Pose des problème de synchronisation et n'est utilisé que sur des courtes distances (bus par exemple).

Transmission Série

- Les bits sont envoyés les uns derrière les autres de manière synchrone ou asynchrone
  - Synchrone : l'émetteur et le récepteur se mettent d'accord sur une base de temps (un top d'horloge) qui se répète régulièrement durant tout l'échange.
    - A chaque top d'horloge (ou *k* tops d'horloge) un bit est envoyé et le récepteur saura ainsi quand lui arrive les bits.
  - Asynchrone : il n'y a pas de négociations préalables
    - Chaque caractère envoyé est précédé d'un bit de start et immédiatement suivi d'un bit de stop.
    - Ces deux bits spéciaux servent à caler l'horloge du récepteur pour qu'il échantillonne le signal qu'il reçoit afin d'y décoder les bits qu'il transmet.

Débits

- Quel que soit le mode de transmission retenu, l'émission est toujours cadencé par une horloge dont la vitesse donne le débit de la ligne en :
  - Bauds : le nombre de tops d'horloge en une seconde.
- Une ligne d'un débit de 100 bauds autorise 100 émissions par seconde.
  - Si à chaque top d'horloge un signal représentant 0 ou 1 est émis :
    - le débit en bits/s est équivalent au débit en baud

Débits

- Un signal émis peux prendre plusieurs valeurs distinctes
  - Exemple : 4 valeurs (0, 1, 2 ou 3)
  - Signal avec une valence de 2
  - Le débit en bit/s est double de celui en baud.
- D'une manière générale, si le signal prend 2^n valeurs distinctes on dit alors que sa valence est de n,
  - A chaque top, n bits peuvent être transmis simultanément
  - Si le débit de la ligne est de x bauds alors il est en $n \, . \, x \ bits/s$

Transmission en bande de base

- Les bits à transmettre doivent être représentés sous forme de signaux électriques
- La méthode la plus simple est de considérer qu'un courant nul indique un 0 et un courant positif un 1
  - Méthode dite transmission en bande de base
  - Génère un signal en forme de créneaux, appelé parfois signal carré
  - Avantages
    - Signal facile à réaliser
    - Ne demande que des équipements simples et peu coûteux, à l'émission comme à la réception
  - Inconvénients
    - Dégradation très rapide des signaux en fonction de la distance parcourue
    - Doivent être utilisés que sur courtes distances ou être régénérés périodiquement sur une distance plus longue

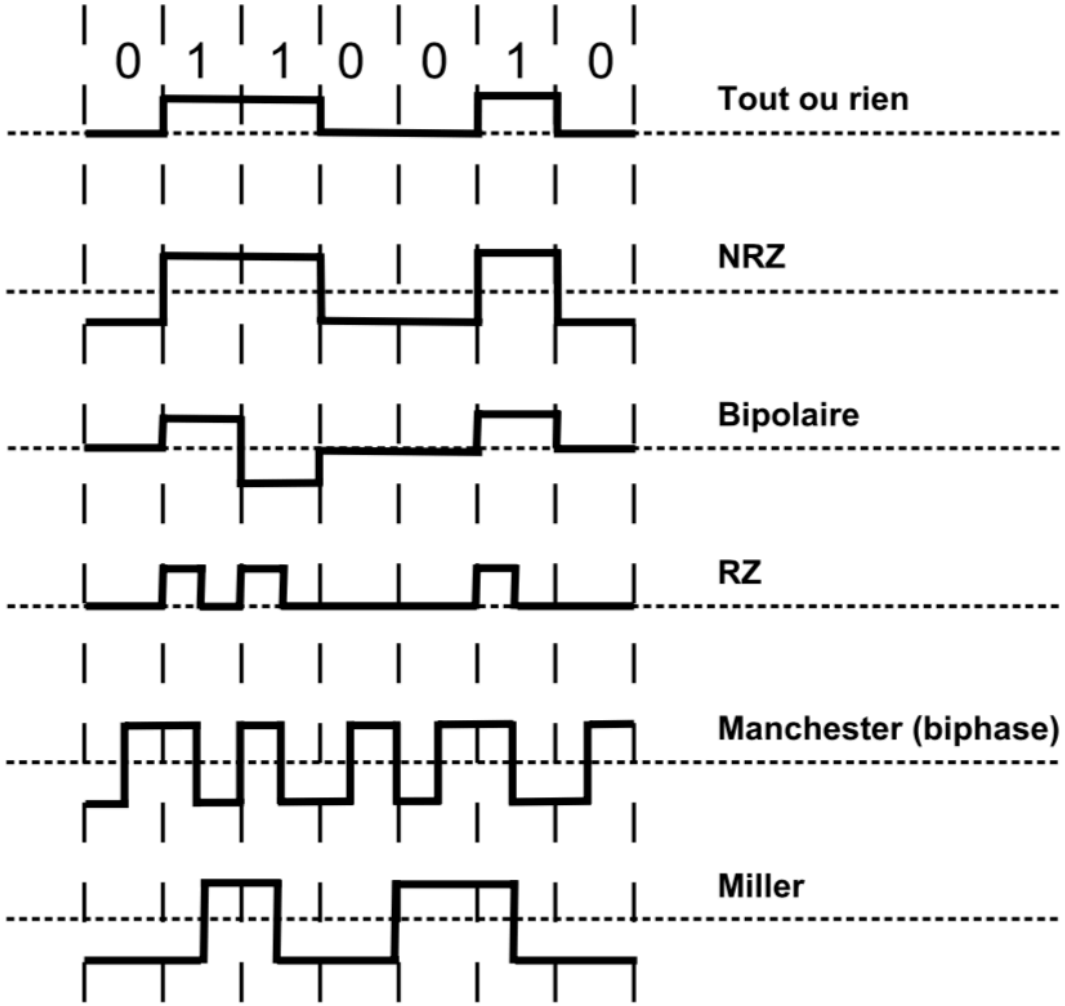
Transmission en bande de base

- le code tout ou rien : c'est le plus simple, un courant nul code le 0 et un courant positif indique le 1
- le code NRZ (non retour à zéro) : pour éviter la difficulté à obtenir un courant nul, on code le 1 par un courant positif et le 0 par un courant négatif
- le code bipolaire : le 0 est représenté par un courant nul, le 1 est représenté par un courant alternativement positif ou négatif pour éviter de maintenir les courants continus

Transmission en bande de base

- le code RZ : le 0 est codé par un courant nul et le 1 par un courant positif qui est annulé au milieu de l'intervalle de temps prévu pour la transmission d'un bit
- le code Manchester : le signal change au milieu de l'intervalle de temps associé à chaque bit. Pour coder un 0 le courant sera négatif sur la première moitié de l'intervalle et positif sur la deuxième moitié, pour coder un 1, c'est l'inverse.
- le code Miller : on diminue le nombre de transitions en effectuant une transition (de haut de bas ou l'inverse) au milieu de l'intervalle pour coder un 1 et n'effectuant pas de transition pour un 0 suivi d'un 1. Une transition est effectuée en fin d'intervalle pour un 0 suivi d'un autre 0.

Transmission en bande de base



Transmission modulée

- Le principal problème de la transmission en bande de base est la dégradation du signal très rapide en fonction de la distance parcourue

- Sur les longues distances, on émet un signal sinusoïdal qui, même s'il est affaibli, sera facilement décidable par le récepteur.

- Ce signal sinusoïdal est obtenu grâce à un modem (modulateur-démodulateur)
  - Prendre en entrée un signal en bande de base pour en faire un signal sinusoïdal (modulation)
  - Restituer un signal carré à partir d'un signal sinusoïdal (démodulation).
  - Autrement dit il permet de passer des signaux numériques discrets (0 et 1) à des signaux analogiques continus.

Transmission modulée

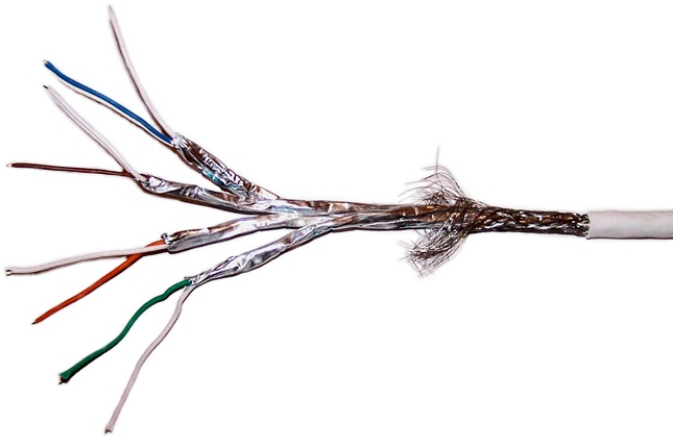
- La modulation d'amplitude envoie un signal d'amplitude différente suivant qu'il faut transmettre un 0 ou un 1. Par contre, il existe des possibilités de perturbation (orage, lignes électriques, etc.), car si un signal de grande amplitude (représentant un 1) est momentanément affaibli le récepteur l'interprétera à tort en un 0.
- La modulation de fréquence envoie un signal de fréquence plus élevée pour transmettre un 1. Comme l'amplitude importe peu, c'est un signal très résistant aux perturbations (la radio FM est de meilleure qualité que la radio AM) et c'est assez facile à détecter.
- La modulation de phase change la phase du signal (de 180^o par exemple) suivant qu'il s'agit d'un 0 (phase montante) ou d'un 1 (phase descendante).

Les supports de transmission

- Câble coaxial
  - constitué d'un coeur qui est un fil de cuivre.
  - Ce coeur est dans une gaine isolante elle-même entourée par une tresse de cuivre,
  - le tout est recouvert d'une gaine isolante.
  - On le rencontre dans sa version 10 Base 2 (ou Ethernet fin 10 Mbits/s sur 200m maximum) ou 10 Base 5 (ou Ethernet épais 10 Mbits/s sur 500m maximum) pour la réalisation de réseaux locaux à topologie en bus.

Les supports de transmission

- Paire torsadée
  - Formée de paires de fil conducteur, contenues dans une gaine isolante
  - Les paires sont torsadées pour éviter les interférences électriques
  - Il existe 5 catégories principales de paires torsadées (3 à 7) avec des débits allant de 10 Mbits/s (10 Base T : 10 pour 10 Mbits/s et T pour Twisted) jusqu'à 10 Gbits/s. Chaque extrémité d'un câble coaxial est muni d'une prise RJ45.



Les supports de transmission

- La fibre optique
  - Le transport d'informations est réalisé par propagation d'ondes lumineuses
  - propagation effectuée par réflexion sur les parois de la fibre
  - diamètre de la fibre compris entre quelques dizaine de microns et quelques centaines de microns
  - Selon le type de fibre, une diode électroluminescente (LED), une diode à infrarouge ou un laser convertit le signal électrique à transmettre en un signal optique
  - Un détecteur de lumière, une photodiode, effectue la conversion inverse
  - La présence ou l'absence d'un signal lumineux permet le codage d'un bit
  - Débits très élevés

Les supports de transmission

- Liaison sans fil
  - Les liaisons sans fil sont possibles grâce à des liaisons infrarouges, laser ou hertziennes sur des courtes distances et grâce aux faisceaux hertziens pour les liaisons satellitaires.
  - Débits sont élevés mais les transmissions sont sensibles aux perturbations et les possibilités d'écoute sont nombreuses.

La couche liaison de données

- La couche liaison de données fournit les moyens fonctionnels et procéduraux nécessaires à l'établissement, au maintien et à la libération des connexions de liaison de données entre entités du réseau.
- Elle détecte et corrige, si possible, les erreurs dues au support physique et signale à la couche réseau les erreurs irrécupérables.
- Elle supervise le fonctionnement de la transmission et définit la structure syntaxique des messages, la manière d'enchaîner les échanges selon un protocole normalisé ou non.
- Une connexion de liaison de données est réalisée à l'aide d'une ou plusieurs liaisons physiques entre deux machines adjacentes dans le réseau donc sans noeuds intermédiaire entre elles.

Détection et correction d'erreurs

- Les techniques employées ici reposent sur l'utilisation de codes correcteurs ou codes détecteurs d'erreurs
  - Chacun transforme la suite de bits à envoyer en lui ajoutant l'information de base de bits de redondance ou de bits de contrôle.
  - Le récepteur se sert de cette information ajoutée pour déterminer si une erreur s'est produite et pour la corriger si la technique employée le permet.

Détection et correction d'erreurs

- Code de parité ajoute à chaque bloc de i bits émis un bit de parité de telle sorte que parmi les $i + 1$ bits émis le nombre de bits à 1 soit toujours pair (ou impair).
- Code à redondance cyclique (CRC) ajoutent des bits qui sont des combinaisons linéaires des bits de l'information à transmettre par le biais d'un polynôme générateur
- Le code de Hamming est un code correcteur d'erreurs basé sur la notion de distance de Hamming

A voir en TD

Protocoles de liaison de données

- Le rôle d'un protocole de liaison de données est de fixer comment doivent être réalisées les différentes tâches qui incombent à la couche 2 du modèle OSI.
- Deux grandes familles de protocoles :
  - Les procédures orientées caractères (par exemple, BSC chez IBM) sont assez anciennes et sont utilisées pour les communications à l'alternat sur le principe *send and wait*.
  - Les procédures orientées bits (par exemple HDLC) sont prévues pour des transmissions full-duplex et à haut débit.

Le protocole HDLC

- Le protocole HDLC (High Level Data Link Control) est :
  - orienté bit et définit un ensemble de procédures normalisées par l'ISO
  - communications, aussi bien point à point que multipoint, half ou full-duplex
  - toujours entre une machine primaire et une ou plusieurs machine secondaire.

Le protocole HDLC

- Modes du protocole HDLC :
  - Le mode ABM (Asynchronous Balanced Mode) est un mode de réponse asynchrone équilibré utilisé sur une liaison full-duplex entre 2 machines uniquement (liaison point à point) qui ont chacune le statut de primaire et de secondaire. Ce dernier peut émettre sans la permission du primaire.
  - Le mode NRM (Normal Response Mode) est utilisé sur une liaison half-duplex où le secondaire ne peut transmettre sans l'invitation du primaire.
  - Le mode ARM (Asynchronous Response Mode) est utilisé sur une liaison half-duplex également, mais le secondaire peut émettre sans que le primaire l'ait sollicité. Ceci peut alors provoquer des problèmes si primaire et secondaire veulent simultanément émettre des données.

Le protocole HDLC

- Les trames échangées ont l'allure suivant :

  fanion adresse commande ... données ... contrôle fanion

- Fanion = 01111110
- Types de trames HDLC
  - Les trames d'information contiennent des données à destination ou en provenance des couches supérieures.
  - Les trames de supervision assurent le contrôle d'erreur et de flux.
  - Les trames non numérotées servent à l'initialisation de la liaison et aux problème de reprise sur erreur non réglés à la couche 2.

La couche réseau

- La couche réseau assure toutes les fonctionnalités de relais et d'amélioration de services entre entités de réseau, à savoir :
  - l'adressage,
  - le routage,
  - le contrôle de flux
  - la détection et correction d'erreurs non réglés par la couche de liaison.
- il s'agit de faire transiter une information complète (un fichier par exemple) d'une machine à une autre à travers un réseau de plusieurs ordinateurs.
- Il existe deux grandes possibilités pour établir un protocole de niveau réseau : le mode avec connexion (par exemple la norme X25) et le mode sans connexion (protocole IP, par exemple).

La couche réseau

- La couche réseau assure toutes les fonctionnalités de relais et d'amélioration de services entre entités de réseau, à savoir :
  - l'adressage,
  - le routage,
  - le contrôle de flux
  - la détection et correction d'erreurs non réglés par la couche de liaison.
- il s'agit de faire transiter une information complète (un fichier par exemple) d'une machine à une autre à travers un réseau de plusieurs ordinateurs.
- Il existe deux grandes possibilités pour établir un protocole de niveau réseau : le mode avec connexion (par exemple la norme X25) et le mode sans connexion (protocole IP, par exemple).

Contrôle de flux

- Le contrôle de flux consiste à gérer les paquets pour qu'ils transitent le plus rapidement possible entre l'émetteur et le récepteur. Il cherche à éviter les problème de congestion qui surviennent lorsque trop de messages y circulent. Les techniques employées sont les suivantes :
  - le contrôle par crédits : seuls N paquets sont autorisés à circuler simultanément sur le réseau, donc un paquet ne peut entrer dans le réseau qu'après avoir acquis un jeton qu'il relâche lorsqu'il arrive à destination. Ici tous les jetons sont banalisés et la difficulté réside dans leur distribution correcte aux bonnes portes du réseau pour assurer un fonctionnement optimal.

Contrôle de flux

- Les techniques de contrôle de flux (la suite) :
  - Amélioration de la précédente en fixant des jetons dédiés par noeud d'entrée dans le réseau. Chaque noeud gère avec ses jetons une file d'attente des paquets qu'il émet. Quand un paquet arrive à destination, le récepteur renvoie à l'émetteur le jeton correspondant au paquet reçu.
  - Dans le cadre d'un circuit virtuel (mode avec connexion), on utilise le mécanisme de fenêtres. Les paquets de données sont numérotés modulo 8 et contiennent deux compteur : P(s) un compteur du paquets émis et P(r) un compteur de paquets reçus. L'émetteur n'est autorisé à émettre que les paquets inclus dans la fenêtre, c'est à dire, les paquets dont le compteur est tel que : Dernier $P(r)$ reçu $\leq P(s)$ courant $\leq$ Dernier $P(r)$ reçu+W

Le routage

- Le routage de paquets dans un réseau maillé consiste à fixer par quelle ligne de sortie chaque noeud réexpédie les paquets qu'il reçoit.
- Ceci se fait en fonction de la destination finale du paquet et selon une table de routage qui indique pour chaque destination finale quelles sont les voies de sortie possibles

Destination finale	Voie de sortie
D1	A_1, A_2
D2	A_2
D3	A_2, A_3
D4	A_3

- De manière générale, le routage est un ensemble de processus algorithmiques devant prendre des décision dispersées dans le temps et dans l'espace. Les différents algorithmes sont répartis sur chaque noeud du réseau et l'ensemble peut fonctionner de manière centralisée ou répartie.

Le routage centralisé

- Il est géré par un noeud particulier du réseau qui reçoit les informations de chacun des noeuds du réseau et leur envoie leur table de routage.
- Pour fixer ces tables, on prend en compte notamment :
  - le coût des liaisons, le coût de passage dans un noeud, le débit demandé, le nombre de noeuds à traverser, la sécurité de transport de certains paquets, l'occupation des mémoires des noeuds de commutation (en charge de routage), etc.
- Le plus souvent un algorithme de plus court chemin donne de bons résultats en fixant à 1 le coût de franchissement d'un noeud (on peut également pondérer plus fortement les noeuds qui sont les plus occupés).

Le routage décentralisé

- Il ne possède pas de centre de contrôle et les règles de passage d'un paquet sont :
  - L'inondation : à la réception d'un paquet, celui-ci est renvoyé sur toutes les lignes de sortie.
  - La technique hot potatoes : un paquet reçu est renvoyé le plus tôt possible par la première sortie vide
  - Le routage adaptatif dans l'espace et dans le temps : demande de la part de chaque noeud, une connaissance complète du réseau. Les différents noeuds s'échangent donc des messages, mais si chacun envoie des messages à tous les autres alors le trafic va augmenter de manière beaucoup trop grande. C'est pourquoi un noeud ne transmet un compte rendu qu'à ses voisins immédiats qui doivent en tenir compte dans leur propre compte rendu.

Le problème de congestion

- Les problèmes de congestion arrivent lorsque les noeuds d'un réseau saturent leurs files d'attente et donc perdent des paquets.
- Si les paquets sont réexpédiés ou si des messages de gestion de réseau se mettent à circuler en grand nombre les performances du réseau vont s'écrouler très vite.
- On essaye d'éviter le problème de congestion en autorisant un paquet à ne rester dans le réseau qu'un temps limité par un temps maximal fixé par le gestionnaire du réseau.
- Tout paquet est donc émis avec la date fixée par une horloge commune au réseau :
  - si un noeud s'aperçoit que le temps de présence dans le réseau d'un paquet est dépassé, il le détruit.
  - Cela permet ainsi que détruire les paquets perdus par erreur d'adressage ou de routage, ainsi que ceux bloqués dans un noeud.
- Cette méthode est assez difficile à mettre en oeuvre et on utilise souvent une méthode plus simple
  - mémoriser simplement dans la zone de temps un nombre décrémenté à chaque traversée de noeud. Lorsque ce temps atteint 0 il est détruit.

La couche transport

- Les La couche transport assure un transfert de données transparent entre entités de session et en les déchargeant des détails d'exécution.
- Elle a pour rôle d'optimiser l'utilisation des services de réseau disponibles afin d'assurer au moindre coût les performances requises par la couche session.
- C'est la première couche à résider sur les systèmes d'extrémité.
- Elle permet aux deux applications de chaque extrémité de dialoguer directement et indépendamment de la nature des sous-réseaux traversés et comme si le réseau n'existait pas.
- Au niveau inférieur de la couche réseau, seule la phase de l'établissement de la liaison logique s'effectue de bout en bout, alors que les transferts d'information se font de proche en proche.
- La couche transport doit assurer, en mode connecté ou non connecté, un transfert transparent de données entre utilisateurs de service réseau en leur rendant la façon dont les ressources de communication sont mises en oeuvre.

La couche session

- Elle fournit aux entités de la couche présentation les moyens d'organiser les dialogues et les échanges de données.
- Une session peut par exemple être utilisée pour la connexion à distance d'un terminal à un ordinateur ou pour le transfert d'un fichier et ceci en mode connecté.
- Bien que très similaires, la session et la connexion de transport ne sont pas identiques. Trois cas de figues peuvent se présenter :
  - Il y a une correspondance exacte entre une session et une connexion de transport.
  - Plusieurs sessions successives sont établies sur une seule et même connexion de transport. Par exemple, ceci peut être utilisé dans le contexte d'une agence de voyage dans laquelle chaque employé utilise un terminal relié à un ordinateur local.
  - Plusieurs connexions de transport successives sont nécessaires pour une seule et même session. Ceci peut arriver lorsqu'une connexion de transport tombe en panne, la couche session établit alors une nouvelle connexion de transport de manière à poursuivre la connexion commencée.
- Le transfert de données : établissement de la session, transfert de données et libération de la session.

La couche présentation

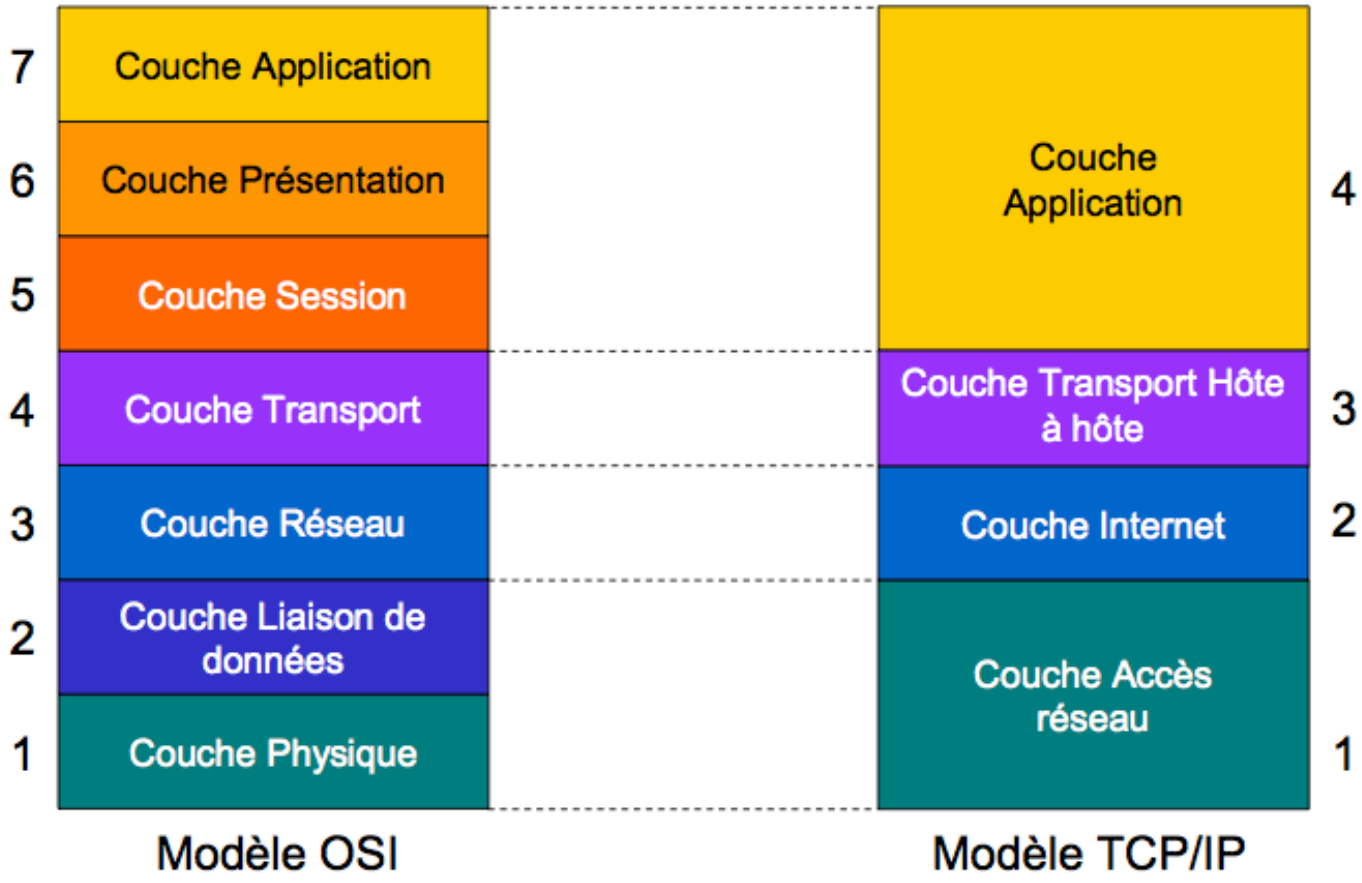
- La couche présentation s'occupe de la syntaxe et de la sémantique des informations transportées en se chargeant notamment de la représentation des données.
  - Par exemple, sur un ordinateur à base de la famille Motorola 68000 les entiers sont représentés avec les bits de poids fort à gauche et ceux de poids faible à droite. Or, c'est l'inverse sur un ordinateur basé sur un processeur de la famille Intel 80x86.
  - L'ISO a défini une norme appelée syntaxe abstraite numéro 1 (Abstract Syntax Notation 1) permettant de définir une sorte de langage commun (une syntaxe de transfert) dans lequel toutes les applications représentent leurs données avant de les transmettre.
- C'est aussi à ce niveau de la couche présentation que peuvent être implémentées des techniques de compression et de chiffrement de données

La couche application

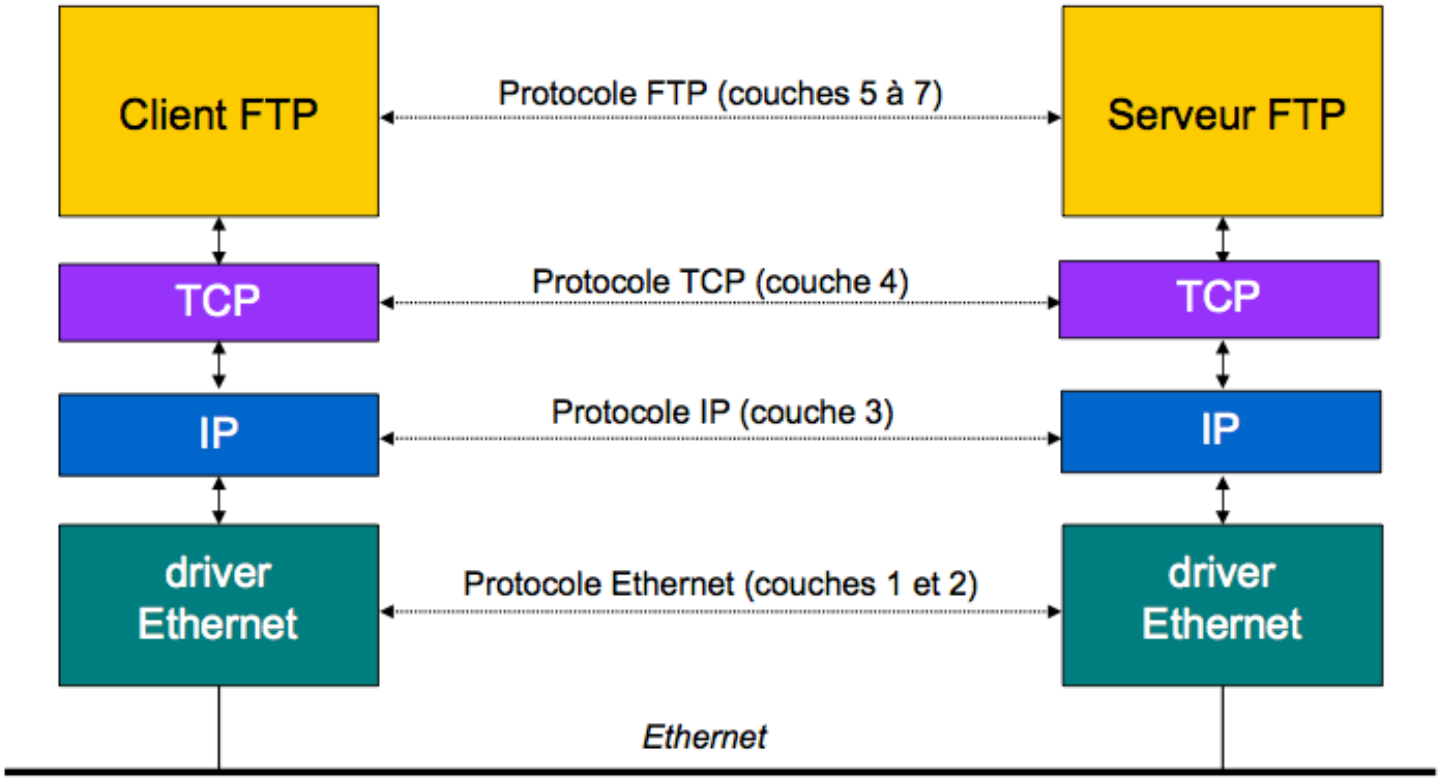
- La couche application donne au processus d'application le moyen d'accéder à l'environnement OSI et fournit tous les services directement utilisables par l'application :
  - l'allocation de ressources
  - l'intégration et la cohérence des données
  - la synchronisation des applications coopérantes
- En fait, la couche application gère les programmes de l'utilisateur et définit des standards pour que les différents logiciels commercialisés adoptent les mêmes principes, comme par exemple :
  - Notion de fichier virtuel représenté sous forme d'arbre pour les applications de transfert de fichiers, opérations permises sur un fichier, accès concurrentiels, etc.
  - Découpe des fonctions d'une application de courrier électronique qui se compose d'un contenu (en-tête et corps) et d'une enveloppe. Une fonctionnalité de l'application gère le contenu et une autre le transfert en interprétant l'enveloppe.

La pile TCP/IP

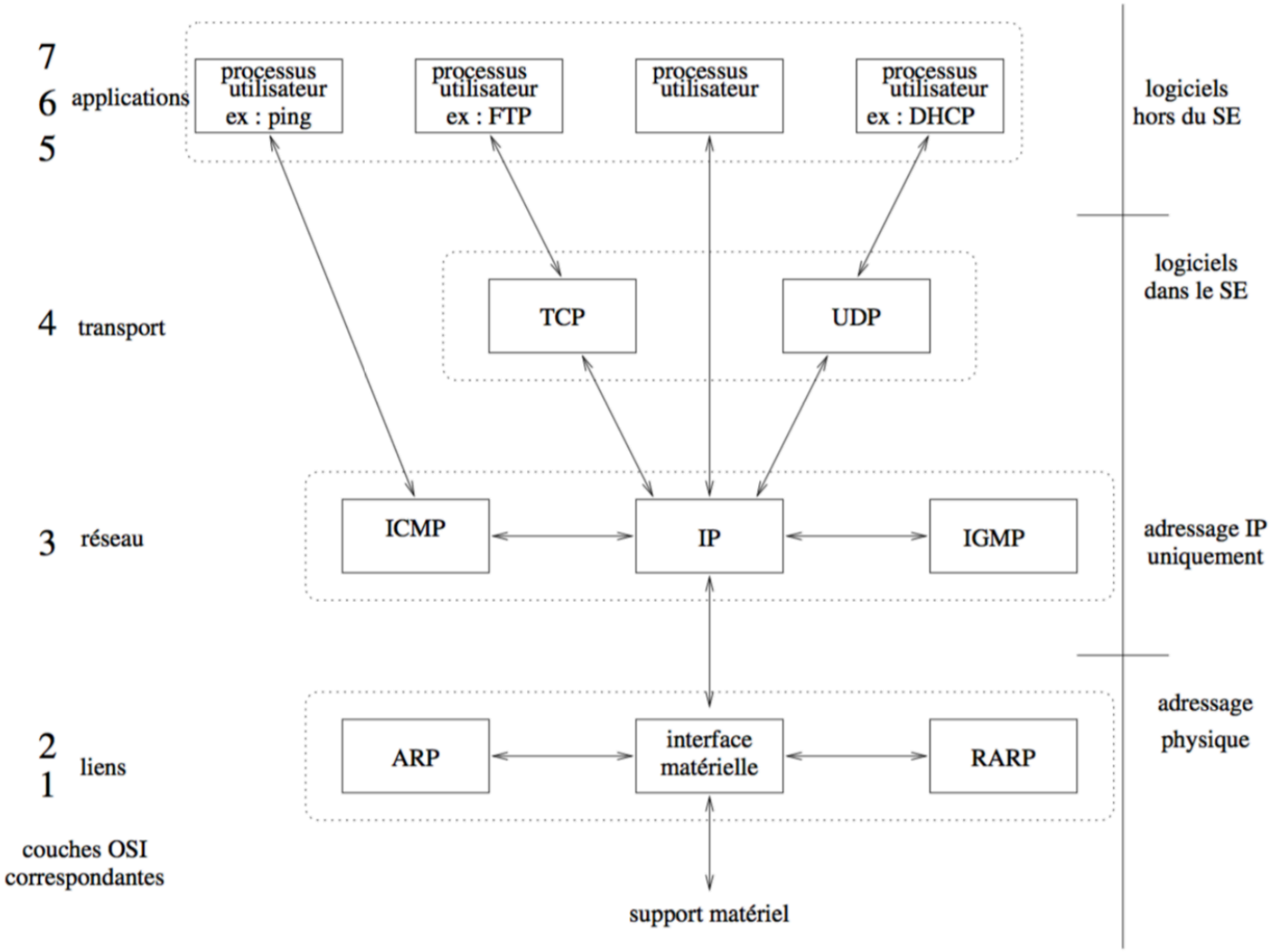
Modèle OSI - TCP/IP



Organisation en couches



Architecture des protocoles TCP/IP



La couche de liens d'Internet

- Le but de la couche de liens de la pile TCP/IP est :
  - d'envoyer et recevoir des datagrammes IP pour la couche IP,
  - d'envoyer des requêtes ARP (resp. RARP)
  - de recevoir des réponses pour le module ARP (resp. RARP).
- Elle concentre donc les caractéristiques des deux premières couches du modèle OSI :
  - couche physique et couche de liaison.

Adresses Ethernet

- Les adresses physiques Ethernet ou MAC adresses (Medium Access control) sont codées sur 6 octets et données sous la forme de 6 nombres hexadécimaux.
- Censées être uniques car les constructeurs et l'IEEE gèrent cet adressage de manière à ce que deux cartes réseaux ne portent pas la même adresse.
- Elles sont de trois types :
  - unicast dans le cas d'une adresse monodestinataire désignant une seule carte réseau,
  - broadcast dans le cas d'une adresse de diffusion générale (tous les bits à 1 donc égale à FF:FF:FF:FF:FF:FF) qui permet d'envoyer une trame à toutes les stations du réseau,
  - multicast dans le cas d'une adresse multidestinataire qui permet d'adresser une même trame à un ensemble de stations qui ont convenu de faire partie du groupe que représente cette adresse multipoint.

Adresses Ethernet

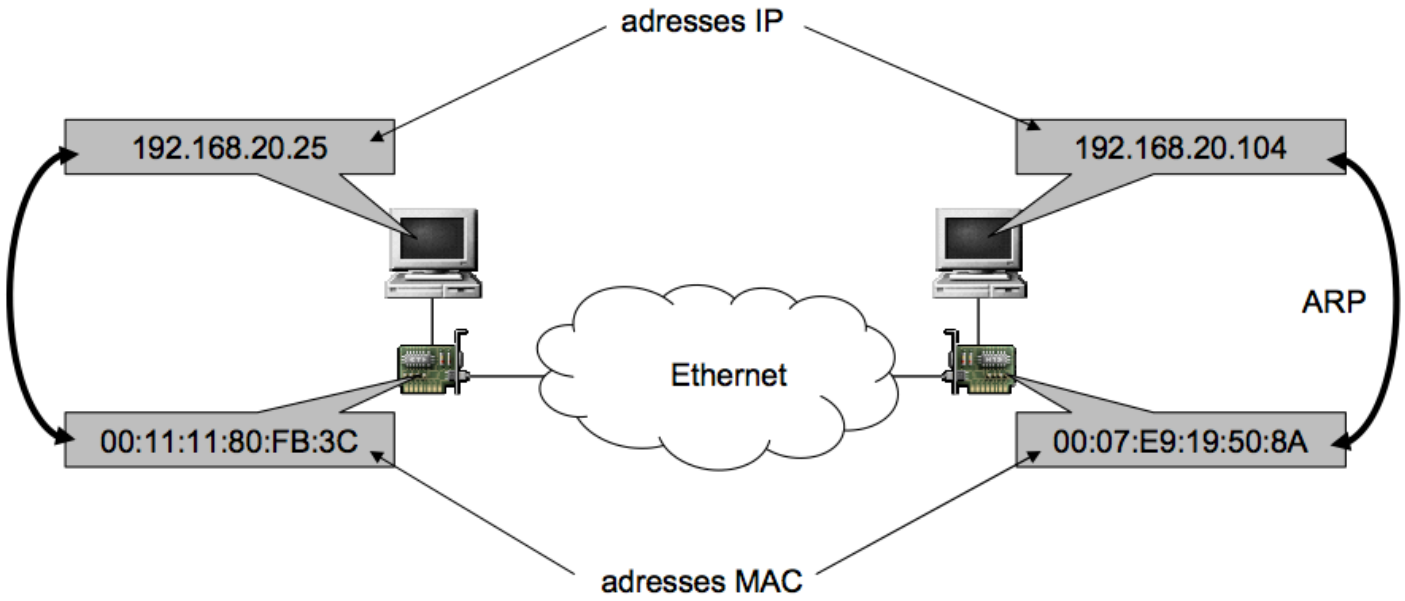
- Une carte réseau doit être capable de reconnaître sa propre adresse physique, l'adresse de multicast, et toute adresse de groupe dont elle fait partie.
- Au niveau des trames, plusieurs formats ont été définis, mais le plus courant aujourd'hui est celui dit de type II illustré dans Figure suivante :

adresse de destination	adresse source	type	données	CRC
6	6	2	46–1500	4

- Les adresses matérielles source et destination sont codées sur 6 octets (adresse Ethernet),
- le troisième champ contient le type de données transmises selon que c'est un datagramme IP, une requête ou réponse ARP ou RARP.
- Les données transmises qui peuvent avoir une taille allant de 46 à 1500 octets.
- Dans le cas de données trop petites, comme pour les requêtes et réponse ARP et RARP on complète avec des bits de bourrage ou padding.
- Enfin, un CRC de 4 octets termine la trame, ce CRC est calculé à partir du polynôme générateur
  $P(x) = x^{32} + x^{26} + x^{23} + x^{22} + x^{16} + x^{12} + x^{11} + x^{10} + x^8 + x^7 + x^5 + x^4 + x^2 + x + 1$

Le protocole ARP

- Le protocole ARP (Address Resolution Protocol)
  - Fournit une correspondance dynamique entre une adresse IP et l'adresse matérielle

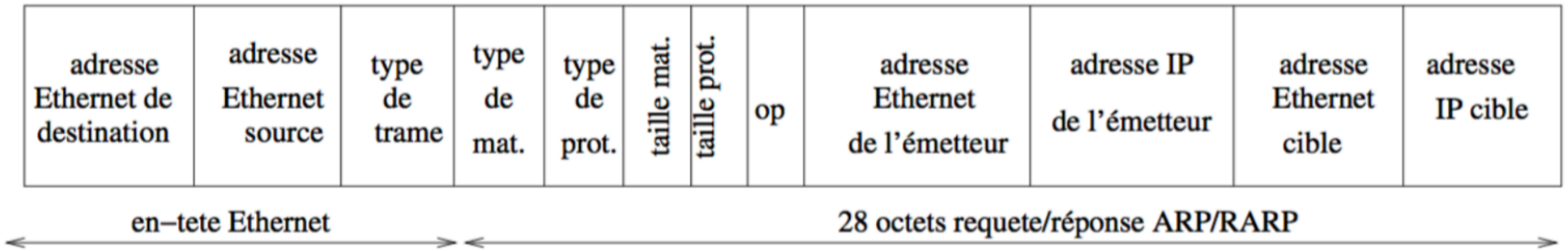


Le protocole ARP

Début d'une connexion FTP entre un PC et un serveur FTP (m.etudes) tous deux à l'intérieur du même réseau Ethernet.

1. Le client FTP convertit l'adresse du serveur FTP en une adresse IP (172.20.41.7) à l'aide du fichiers /etc/hosts ou d'un serveur de noms (DNS).
2. Le client FTP demande à la couche TCP d'établir une connexion avec cette adresse.
3. TCP envoie une requête de connexion à ce serveur en émettant un datagramme IP contenant l'adresse IP.
4. En supposant que les machines client et serveur sont sur le même réseau local Ethernet, la machine émettrice doit convertir l'adresse IP sur 4 octets en une adresse Ethernet sur 6 octets avant d'émettre la trame Ethernet contenant le paquet IP. C'est ce que va faire ARP.
5. Le module ARP envoie une requête ARP dans une trame Ethernet avec une adresse de destination multicast. Ainsi, toutes les machines du réseau local reçoivent cette requête contenant l'adresse IP à résoudre.
6. La couche ARP de la machine visée reconnaît que cette requête lui est destinée et répond par une réponse ARP contenant son adresse matérielle 00:20:AF:AB:42:43. Les autres machines du réseau ignorent la requête.
7. La réponse ARP est reçue par l'émetteur de la requête. Pour ce retour, il n'y a pas de problème de résolution puisque l'adresse physique de l'émetteur étant envoyée dans la requête elle est connue de la machine qui répond.
8. La réponse ARP est reçue par la couche ARP du client FTP, et le driver Ethernet peut alors émettre le paquet IP avec la bonne adresse Ethernet de destination.

Le protocole ARP



- La valeur du champ type de trame est 0806 indiquant le protocole ARP.
- Le champ type de matériel est égal à 1 pour un réseau Ethernet
- Le champ type de protocole est égal est 0800 pour IP.
- Les tailles en octets spécifiées ensuite sont 6 (6 octets pour une adresse Ethernet) et 4 (4 octets pour une adresse IP).
- Le champ op vaut 1 pour une requête ARP et 2 pour une réponse ARP.

Le protocole ARP

- Pour éviter la multiplication des requêtes ARP, chaque machine gère un cache dans lequel elle mémorise les correspondances adresses IP/adresses Ethernet déjà résolues préalablement.
- Le module ARP ne lancera une requête que lorsqu'il ne trouvera pas cette correspondance dans le cacheL
- Les correspondances ne sont pas conservées indéfiniment car cela pourrait provoquer des erreurs lorsque l'on change un ordinateur (ou une carte réseau) du réseau en conservant un même numéro IP pour cet ordinateur mais évidemment pas la même adresse physique.

Le protocole RARP

- Le protocole RARP joue le rôle inverse de ARP en permettant de déterminer l'adresse IP d'un équipement dont on connaît l'adresse physique.
- Le format d'une trame RARP est identique que pour ARP
  - le champ type de trame vaut 0835 et le champ
  - op vaut 3 pour une requête RARP et 4 pour une réponse.
  - Une requête RARP est diffusée sous forme de broadcast, donc toutes les machines du réseau la reçoivent et la traitent.
  - La plupart des machines ignorent simplement cette demande, seuls, le ou les serveurs RARP du réseau vont traiter la requête grâce à un ou plusieurs fichiers et vont retourner une réponse contenant l'adresse IP demandée.

Le protocole IP

- Le Le protocole IP (Internet Protocol, RFC 791) est au coeur du fonctionnement d'internet.
- Il assure sans connexion un service non fiable de délivrance de datagrammes IP.
- Le service est non fiable car il n'existe aucune garantie pour que les datagrammes IP arrivent à destination.
- Certains peuvent être perdus, dupliqués, retardés, altérés ou remis dans le désordre.
- On parle de remise au mieux (best effort delivery) et ni l'émetteur ni le récepteur ne sont informés directement par IP des problèmes rencontrés.
- Le mode de transmission est non connecté car IP traite chaque datagramme indépendamment de ceux qui le précèdent et le suivent. Ainsi en théorie, au moins, deux datagrammes IP issus de la même machine et ayant la même destination peuvent ne pas suivre obligatoirement le même chemin.

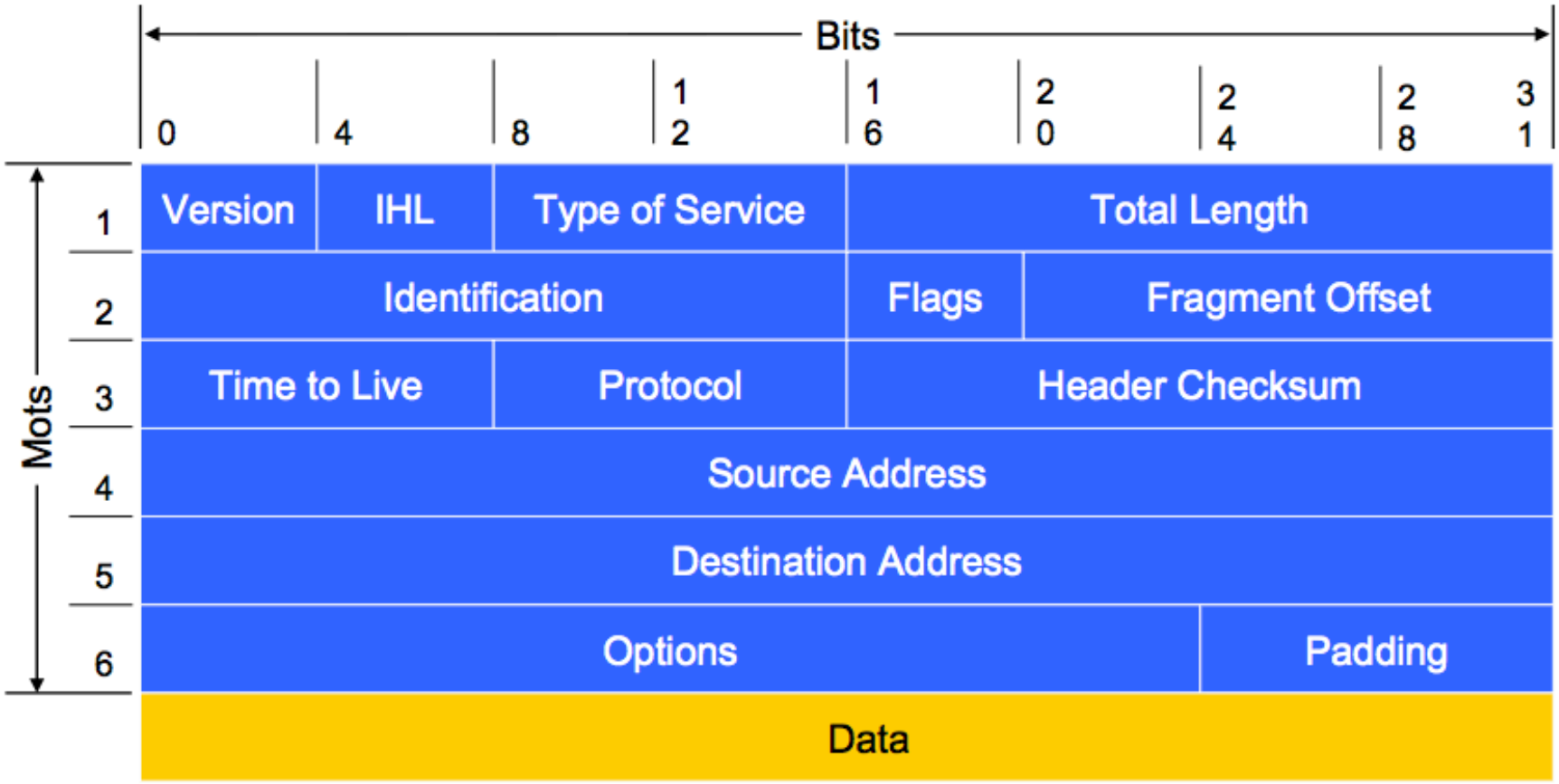
Le protocole IP

- Le rôle du protocole IP est centré autour des trois fonctionnalités suivantes :
  - fournir un service d'adressage logique,
  - définir le format du datagramme IP qui est l'unité de base des données circulant sur Internet,
  - définir le routage dans internet,
  - définir la gestion de la remise non fiable des datagrammes.

Format du datagramme IPv4

- Lors de l'émission, les données sont découpées en petits paquets, appelés datagrammes IP
- Les datagrammes sont tous composés :
  - d'un en-tête
  - suivi d'une zone de données
- L'en-tête contient les adresses de l'émetteur et du destinataire
- Le routage est basé sur l'adresse du destinataire

Format du datagramme IPv4



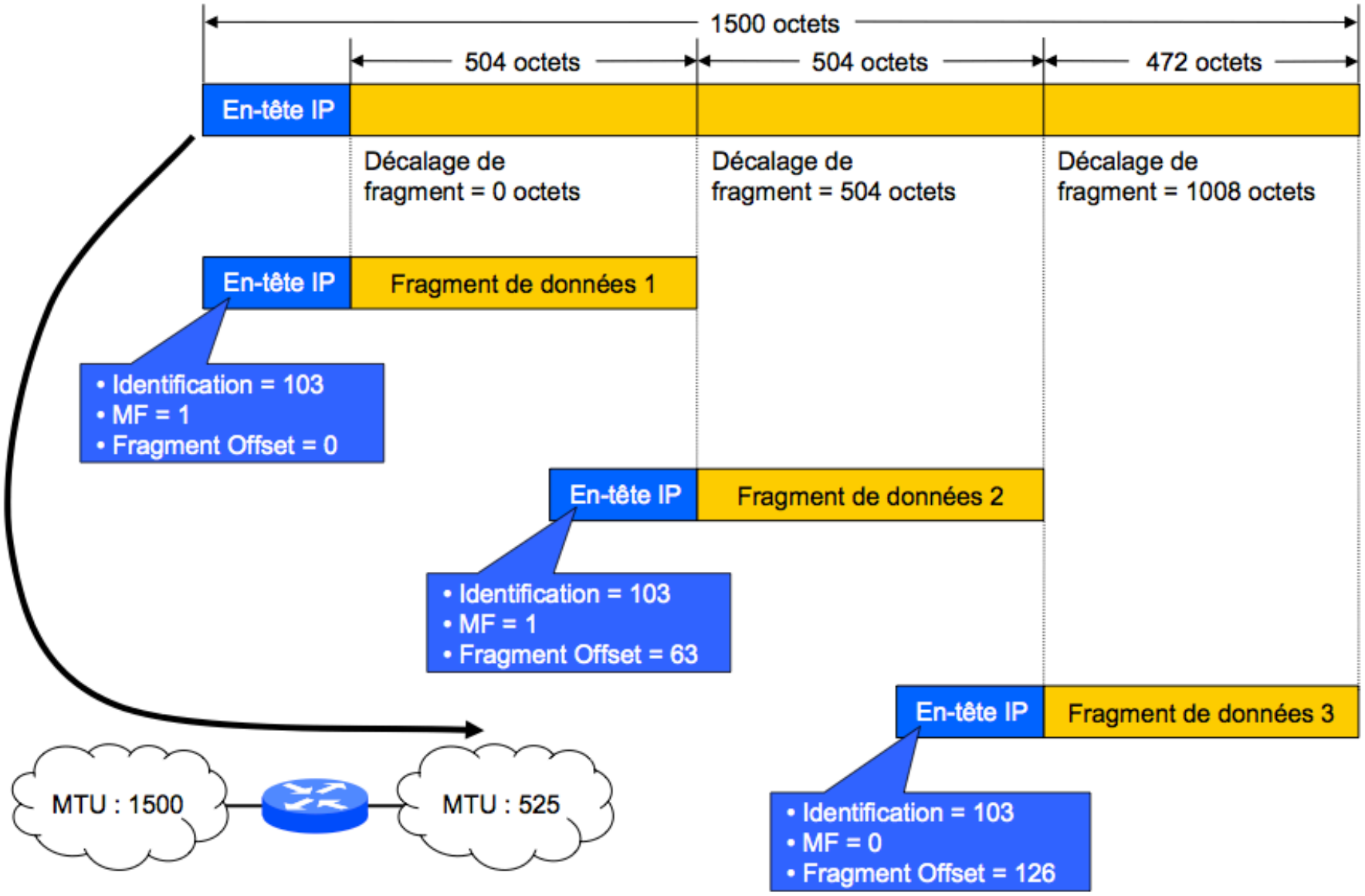
Format du datagramme IPv4

- Par défaut, la longueur de l'en-tête est de 5 mots de 32 bits (soit 20 octets) ; le sixième mot est facultatif. Puisque la longueur de l'en-tête est variable, elle inclut un champ appelé Internet Header Lenght (IHL - longueur de l'en-tête Internet) en mots.
- Le champ Version sur 4 bits indique le format de l'en-tête IP : 4 = version actuel (IPv4) ou 6 = version suivante (IPv6). Il est utilisé par l'émetteur, le récepteur et tout routeur intermédiaire pour déterminer le format de l'en-tête IP.
- Le champ Type of Service (TOS) informe les réseaux de la qualité de service désirée, spécifiant ainsi la préséance, les délais, le débit et la fiabilité. La plupart des implémentations de TCP/IP et des protocoles de routage ignorent ce champ.
- Le champ Total length (longueur totale) contient la longueur de l'en-tête et des données IP, en octets. La durée de vie (Time To Live) représente la durée maximale de vie d'un datagramme sur le réseau. Cette valeur est décrémentée à chaque routeur.
- Si la fragmentation est nécessaire, le champ Identification indique à quel datagramme le fragment appartient, et le champ Fragment Offset (décalage de la fragmentation) précise à quelle partie du datagramme correspond ce fragment. Le champ Flags (Drapeaux) possède un élément binaire " More Fragments bit " qui indique à IP s'il a assemblé tous les éléments du datagramme.
- Le champ Protocol indique quel protocole de couche supérieure recevra les données IP (6 = TCP, 17 = UDP, 1 = ICMP). Sous Unix, ces valeurs sont stockées dans un fichier spécial /etc/protocols
- En IPv6, l'en-tête du datagramme de base ne comprend que 7 champs. Un champ En-tête suivant identifie le prochain en-tête (dans le même datagramme IPv6). Il peut s'agir d'un protocole (de niveau supérieur ICMP, UDP, TCP, ...) ou d'une extension.

Fragmentation

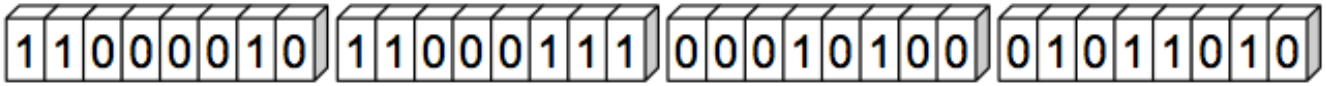
- La fragmentation intervient lorsqu'un datagramme est plus grand que la MTU (Maximum Transfer Unit) supportée par le réseau.
- Exemple : un datagramme de 1500 octet est envoyé sur un réseau Ethernet. En chemin, il doit passer sur une liaison série dont la MTU est de 525 octets. Le datagramme sera alors fragmenté en 3 datagrammes chacun avec une taille < 525 octets. Le message sera réassemblé tout à la fin par le destinataire et non pas par le routeur suivant.

Fragmentation



La structure de l'adresse IPv4

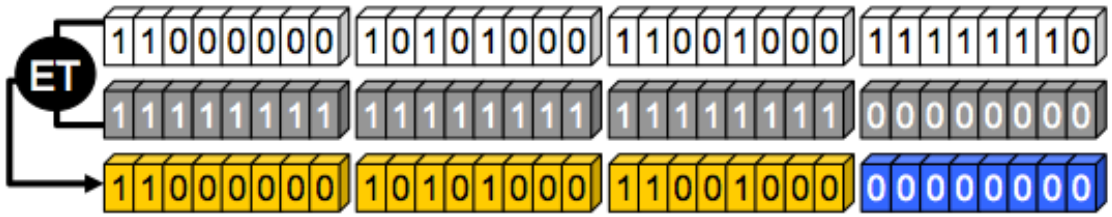
- Chaque interface réseau d'un appareil possède une adresse IP unique au monde
  - Configurable par logiciel
  - Attribuée par le NIC (Network Information Center)
  - Codée sur 32 bits en notation décimale pointée
    - exemple : 194.199.20.90



La structure de l'adresse IPv4

- Adresse hiérarchique
  - Une relation existe entre les adresses d'équipements voisins
- Structurée en deux parties :
  - le préfixe, donnant le numéro de réseau : ID de réseau ou « netid »
  - le suffixe, donnant le numéro de la machine (hôte) dans ce réseau : ID de station ou « hostid »
- Un masque (netmask) est associé à cette adresse
  - il permet au logiciel IP de déterminer le préfixe de réseau d'une adresse en calculant un ET logique avec le masque

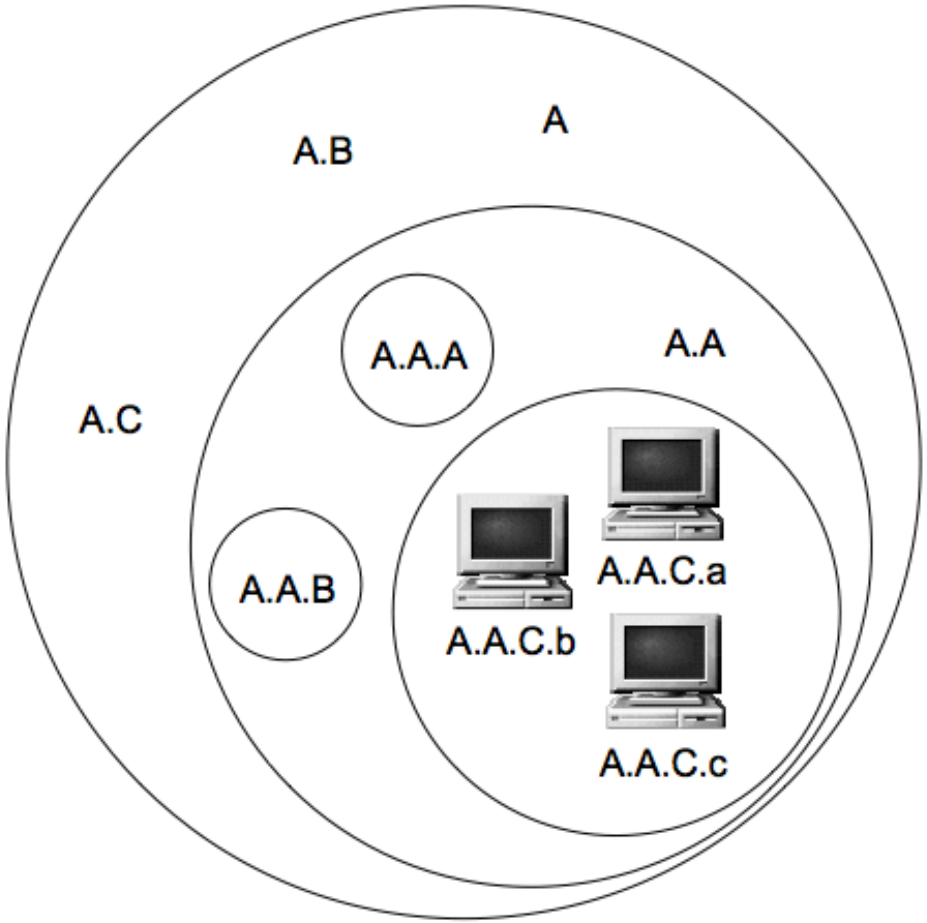
Adresse IP : 192.168.200.254
Masque réseau : 255.255.255.0
Préfixe réseau : 192.168.200.0



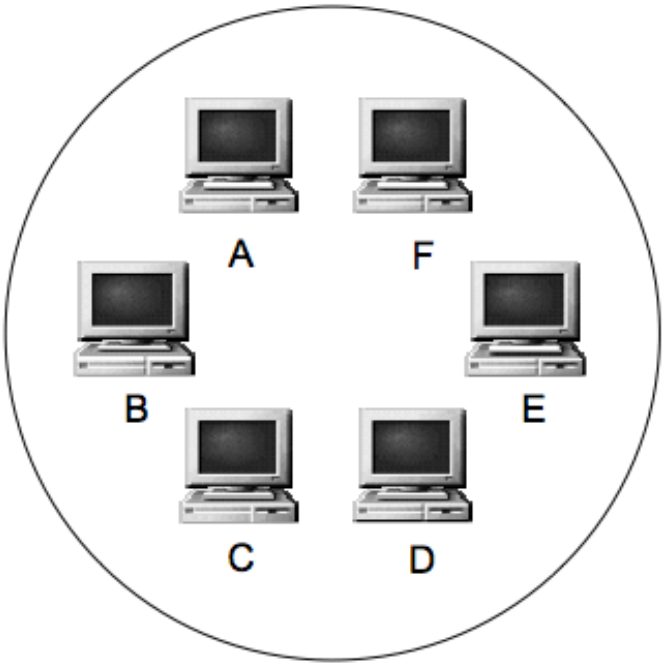
La structure de l'adresse IPv4

- Lorsque le masque est spécifié, on l'écrit généralement sous la forme : adresse IP/masque de réseau, par exemple 192.168.200.254/255.255.255.0
- Il existe également une notation condensée dans laquelle, on écrit l'adresse IP suivie simplement du nombre de bits à 1 du masque, par exemple : 192.168.200.254/24

Espace d'adressage IPv4

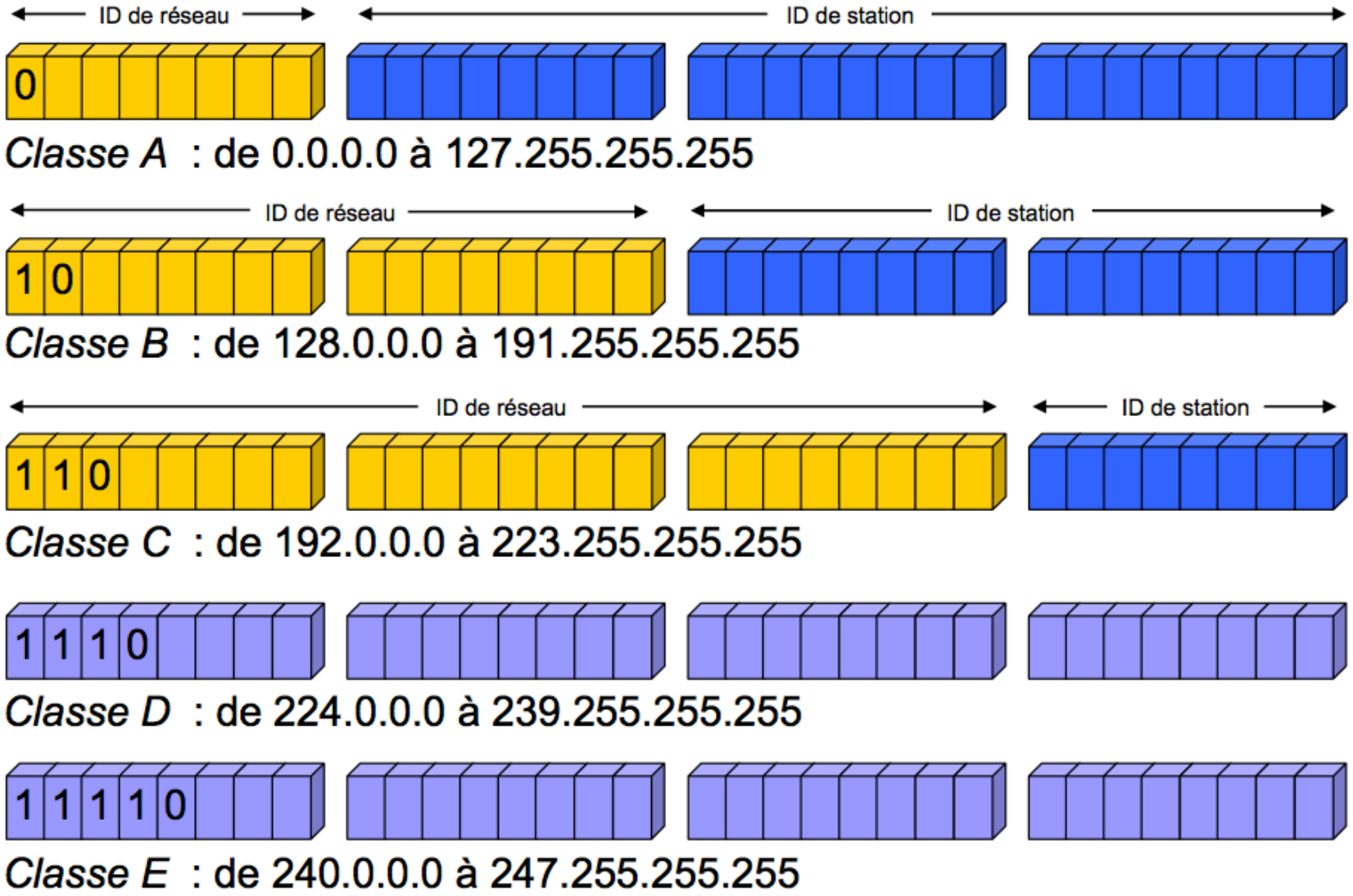


Espace d'adressage hiérarchique



Espace d'adressage plat

Structure de l'adresse IP (v4)
Classes de réseaux



Structure de l'adresse IP (v4)
Classes de réseaux

- Classe A : 1 octet moins le premier bit à 0 pour l'identificateur de réseau
- Classe B : 2 octets moins les 2 premiers bits à 10 pour l'identificateur de réseau
- Classe C : 3 octets moins les 3 premiers bits à 110 pour l'identificateur de réseau
- Classe D : cas particulier, pas de distinction réseau/hôte ; 4 premiers bits à 1110 puis 28 bits pour l'adresse de diffusion de groupe
- Classe E : 5 premiers bits à 11110 puis 27 bits réservés pour une utilisation future

Structure de l'adresse IP (v4)

- Adresse de réseau :
  - Identificateur de réseau suivi de bits à 0
  - Exemples :
    - 125.0.0.0 = réseau 125 de classe A
    - 129.15.0.0 = réseau 129.15 de classe B
    - 192.168.30.0 = réseau 192.168.30 de classe C
- Adresse de diffusion ou broadcast :
  - Identificateur de réseau suivi de bits à 1
    - Exemples :
      - 125.255.255.255 = diffusion sur le réseau 125 de classe A
      - 129.15.255.255 = diffusion sur le réseau 129.15 de classe B
      - 192.168.30.255 = diffusion sur le réseau 192.168.30 de classe C

Adresses IPv4 particulières

- Au lieu d'utiliser un adressage plat (1, 2, 3, etc.) la méthode retenue est plus efficace car elle permet une extraction rapide du numéro de réseau à l'intérieur d'une adresse IP ce qui facilitera le routage.
- Toutes les combinaisons mathématiquement possibles pour identifier un réseau ou une machine ne sont pas permises car certaines adresses ont des significations particulières.
    - 0.0.0.0 est utilisée par une machine pour connaître sa propre adresse IP lors d'une processus d'amorçage par exemple.
    - <id. de réseau nul>.<id. de machine> est utilisée pour désigner une machine sur son réseau lors d'un boot également.
    - <id. de réseau>.<id. de machine nul> n'est jamais affectée à une machine car elle permet de désigner le réseau lui-même.
    - <id. de réseau>.<id. de machine avec tous ses bits à 1> est une adresse de diffusion ou de broadcasting, c'est-à-dire qu'elle désigne toutes les machines du réseau concerné. Un datagramme adressé à cette adresse sera ainsi envoyé à toutes les machines du réseau.
    - 255.255.255.255 est une adresse de diffusion locale car elle désigne toutes les machines du réseau auquel appartient l'ordinateur qui utilise cette adresse. L'avantage par rapport à l'adresse précédente est que l'émetteur n'est pas obligé de connaître l'adresse du réseau auquel il appartient.
    - 127.X.Y.Z est une adresse de rebouclage qui est utilisée pour permettre les communications inter-processus sur un même ordinateur ou réaliser des tests de logiciels car tout logiciel de communication recevant des données pour cette adresse les retourne simplement à l'émetteur.
    - Les adresses des classes : A de 10.0.0.0 à 10.255.255.255, B de 172.16.0.0 à 172.31.255.255 et C de 192.168.0.0 à 192.168.255.255 sont réservées à la constitution de réseaux privés autrement appelés *intranet*

Classless Inter Domain Routing

- Une entreprise veut numéroter 2000 machines ne peut se contenter d'un réseau de classe C. Par contre si on lui attribue un réseau de classe B, on perd plus de 60 000 adresses qui resteront inutilisées !
- Devant la pénurie d'adresses de classes B le système CIDR (Classless Inter Domain Routing : RFC 1518, 1519) est apparu en 1993.
- Une telle adresse CIDR est de la forme **A.B.C.D/M** où **M** est un entier appelé **masque**.
- Ce masque désigne le nombre de bits constituant l'identifiant de réseaux dans l'adresse A.B.C.D.
- Par exemple, dans 172.20.41.7/16, les 16 premiers bits de l'adresse désigne le réseau qui est donc 172.20.0.0 et l'identifiant de machine est 0.0.41.7.
- Le masque, ici égal à 16, peut également être donné sous la forme décimale 255.255.0.0 correspondant à une adresse IP ayant ses 16 premiers bits à 1.
- Étant donné une adresse IP donnée sous la forme CIDR comme 150.50.215.200/21 on retrouve les identifiants de réseau et de machines en effectuant un ET logique entre l'adresse complète et le masque tous les deux mis sous forme binaire.

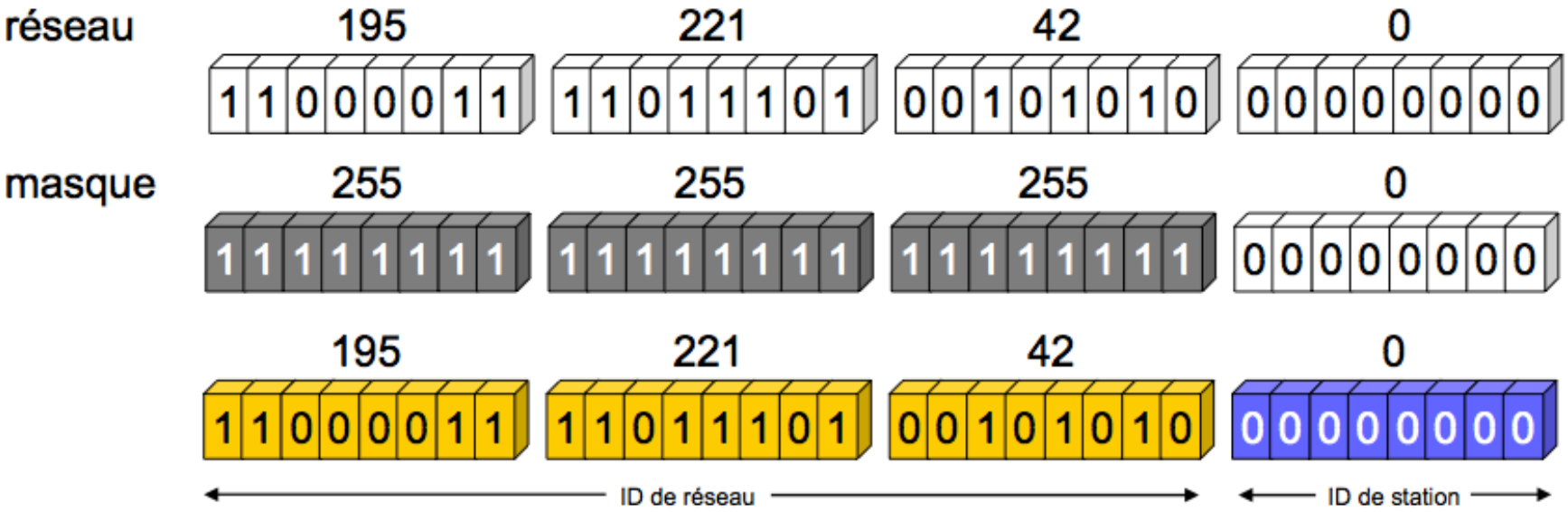
Adressage de sous-réseaux

- Exemple : réseau de classe B 140.30.0.0
  - masque de réseau par défaut 255.255.0.0 si aucun sous- réseau n'est défini
  - masque 255.255.255.0 si présence de (au plus 254) sous- réseaux (de 254 hôtes chacun)

Adressage de sous-réseaux

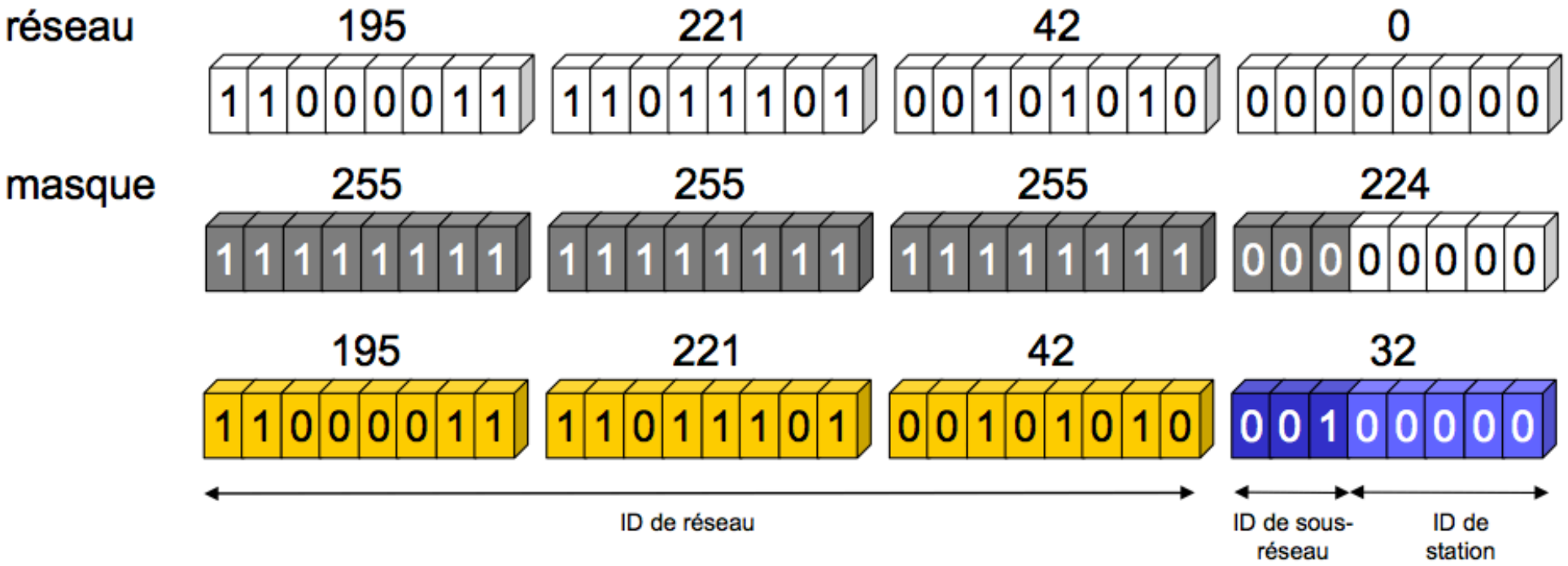
- Le découpage en sous-réseaux est inconnu de l'extérieur
  - Il passe par l'utilisation d'un masque de sous-réseau (subnet mask)
- On utilise la même notation que l'adresse IP :
  - bits réseau à 1
  - bits de la partie sous-réseau à 1
  - bits de la partie "host" à 0

Exemple sans sous-réseaux



- Adresse réseau : 195.221.42.0
- Masque : 255.255.255.0
- Adresses des hôtes : 195.221.42.1 à 195.221.42.254
- Adresse de broadcast : 195.221.42.255

Exemple avec sous-réseaux



DHCP

- De manière administrative, l'obtention d'une plage d'adresses IP pour créer un nouveau réseau est gérée par l'ICANN de manière décentralisée et hiérarchique.
- Par exemple, pour l'Europe, c'est le RIPE Network Coordination Centrequi assure cette gestion.
- D'une manière générale, les FAI (Fournisseurs d'Accès à Internet) disposent ainsi de plages d'adresses qui leurs sont attribuées par l'un de ces organismes

DHCP

- De manière technique, une machine peut avoir une adresse IP statique, qu'elle conserve de manière permanente, ou dynamique, qui change (ou peut changer) à chaque redémarrage ou quand cette adresse n'est plus valide.
- Par ailleurs, l'attribution de cette adresse IP peut être réalisée via une configuration manuelle, ou via le protocole DHCP(Dynamic Host Configuration Protocol).
- DHCP est un protocole client-serveur où le client est une machine qui demande à s'intégrer au réseau IP « géré » par le serveur DHCP.
- La principale phase du protocole se découpe en 4 étapes.
- Tous les messages DHCP d'un client vers un serveur sont envoyés dans des datagrammes UDP adressés au port 67 et les messages d'un serveur vers un client sont envoyés dans des datagrammes UDP adressés au port 68.

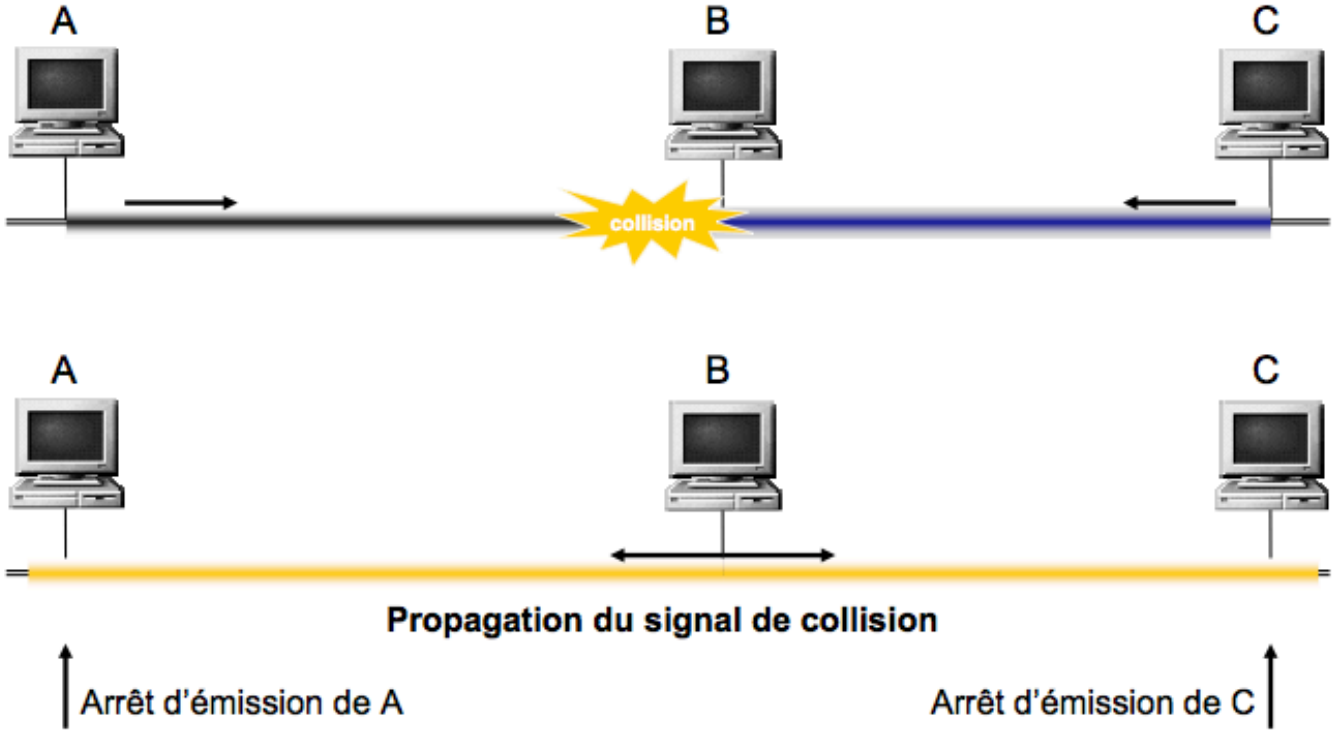
DHCP

- DHCPDISCOVER : le client envoie en diffusion (à l'adresse IP 255.255.255.255) une requête en spécifiant 0.0.0.0 comme adresse IP d'origine puisqu'il ne possède pas d'adresse IP pour l'instant. Il indique aussi son adresse matérielle et un numéro de transaction. Ce message est reçu par toutes les machines du réseau, et notamment par les serveurs DHCP qui vont y répondre.
- DHCPOFFER : les serveurs DHCP répondent par un message contenant l'identifiant de transaction, l'adresse IP proposée, le masque de sous-réseau et la durée du bail (durée de vie de cette adresse avant expiration).
- DHCPREQUEST : le client accepte l'une des propositions (a priori la première) et répond en envoyant en diffusion un message contenant les divers paramètres.
- DHCPACK : le serveur concerné confirme le bail et mémorise de son côté que cette adresse IP est désormais inutilisable jusqu'à sa libération.

DHCP

- Les autres points du protocole sont gérés par les messages suivants :
  - DHCPNACK : le serveur informe le client que le bail est terminé
  - DHCPDECLINE : le client refuse l'adresse IP car elle est déjà utilisée
  - DHCPRELEASE : le client libère l'adresse IP et annule le bail
  - DHCPINFORM : le client possède une IP et il demande des paramètres de configuration locaux

CSMA/CD


A
B
C
collision
A
B
C
Propagation du signal de collision
Arrêt d'émission de A
Arrêt d'émission de C

CSMA/CD

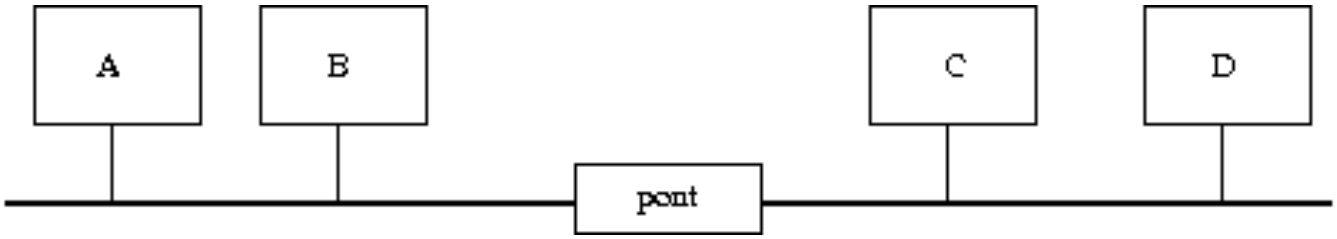
- Comme il n'y a pas d'autorité centrale qui gère l'accès au câble dans une architecture en bus, il est possible que plusieurs stations veuillent émettre simultanément sur le câble.
- C'est pourquoi chaque carte réseau écoute le câble pendant qu'elle émet des données afin de détecter des éventuelles perturbations.
- Si une collision est détectée par une carte réseau, celle-ci arrête d'émettre et attend un laps de temps aléatoire compris entre 0 et une certaine durée δ avant de réémettre ses données.
- S'il y a encore un problème de collision, alors un nouveau temps d'attente est tiré au sort entre 0 et 2δ, puis entre 0 et 4δ, ... jusqu'à ce que la trame soit émise.
- Ce principe est justifié par le fait que si une première collision se produit, il y a de fortes chances que les délais d'attente tirés au sort par chacune des 2 stations soient très proches, donc il ne sera pas surprenant d'avoir une nouvelle collision.
- En doublant à chaque fois l'intervalle des délais d'attente possibles on augmente les chances de voir les retransmissions s'étaler sur des durées relativement longues et donc de diminuer les risques de collision.
- Elle est efficace en général mais a le défaut de ne pas garantir un délai de transmission maximal après lequel on est sûr que la trame a été émise, donc cela ne permet pas de l'envisager pour des applications temps réel.

Quelques équipements

- Un **répéteur** opère de manière physique uniquement, donc au niveau de la couche 1 du modèle OSI. Il se contente de retransmettre et d'amplifier tous les signaux qu'il reçoit, sans aucun autre traitement.
- Un **hub** est un multiport qui renvoie donc le signal qu'il reçoit par l'un de ses ports vers tous ses autres ports.

Quelques équipements

- Un **pont** est un équipement qui intervient dans l'architecture d'un réseau en reliant deux segments disjoints de ce réseau. Le pont appartient à la couche 2 du modèle OSI car il va filtrer les trames du réseau en fonction de leur origine et destination.

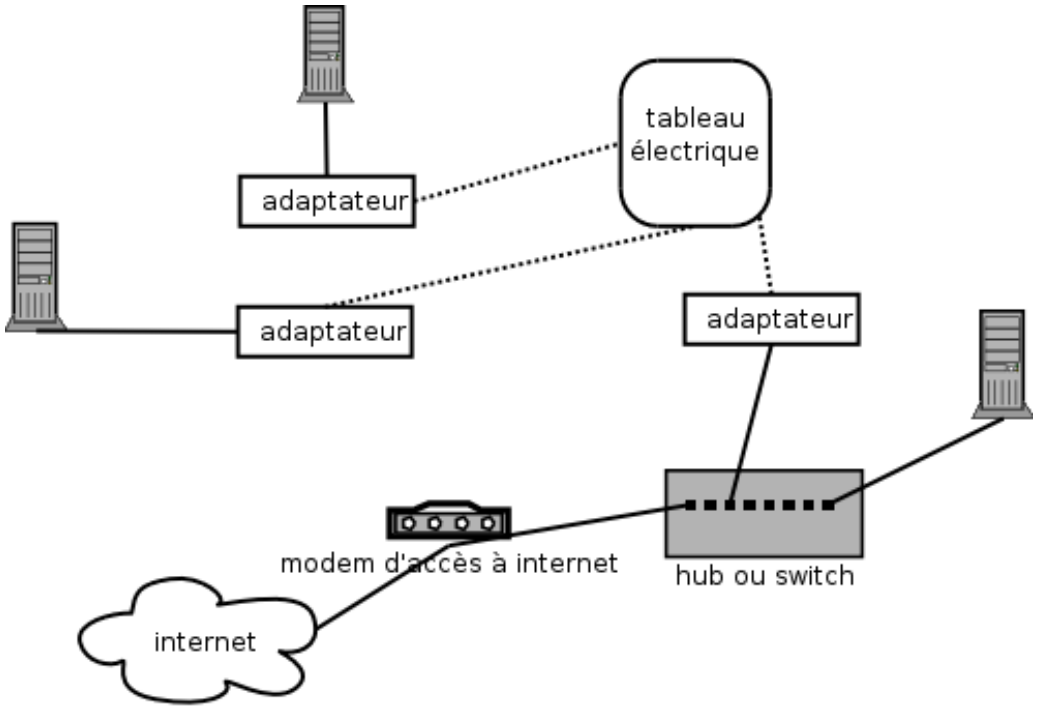


Quelques équipements

- Un **commutateur ou switch** va aiguiller chacune des trames qu'il reçoit vers le segment sur lequel se trouve l'ordinateur de destination de la trame.
  - Chacun de ses ports est habituellement relié à un segment contenant un nombre restreint d'ordinateurs, voire à un seul s'il s'agit par exemple d'un serveur très sollicité.
  - Les performances globales du réseau seront donc bien meilleures que lorsque les postes sont reliés via un hub puisque les changes entre 2 machines du réseau n'inondent pas inutilement les autres machines du réseau.
  - Les meilleures débits et la meilleure confidentialité possibles sur un réseau local Ethernet sont atteints si l'on peut mettre en place un réseau « tout commuté ». Ce terme signifie que chaque poste du réseau est relié par un lien direct à un port du commutateur et ne reçoit ainsi que son trafic personnel.

Quelques équipements

- **La technologie du CPL (Courant Porteur en Ligne)** permet d'étendre un réseau local Ethernet au moyen du réseau électrique interne d'un bâtiment (accès indoor). Cette technique peut aussi s'utiliser pour relier à internet une habitation (accès outdoor). Le réseau électrique se comporte alors comme un bus Ethernet.

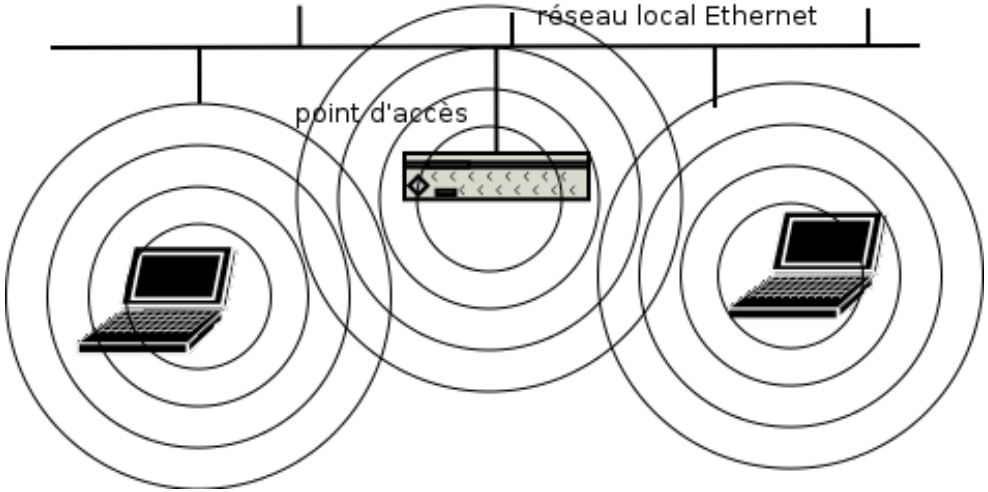


Le réseau Wifi

- La norme IEEE 802.11 définit les caractéristiques d'un réseau local sans fil (WLAN) plus connu sous le nom WIFI (WIreless FIdelity).
- Au niveau physique on distingue 3 modes de communication : IR (infrarouge), DSSS (Direct Sequence Spread Spectrum) et FHSS (Frequency Hopping Spread Spectrum).

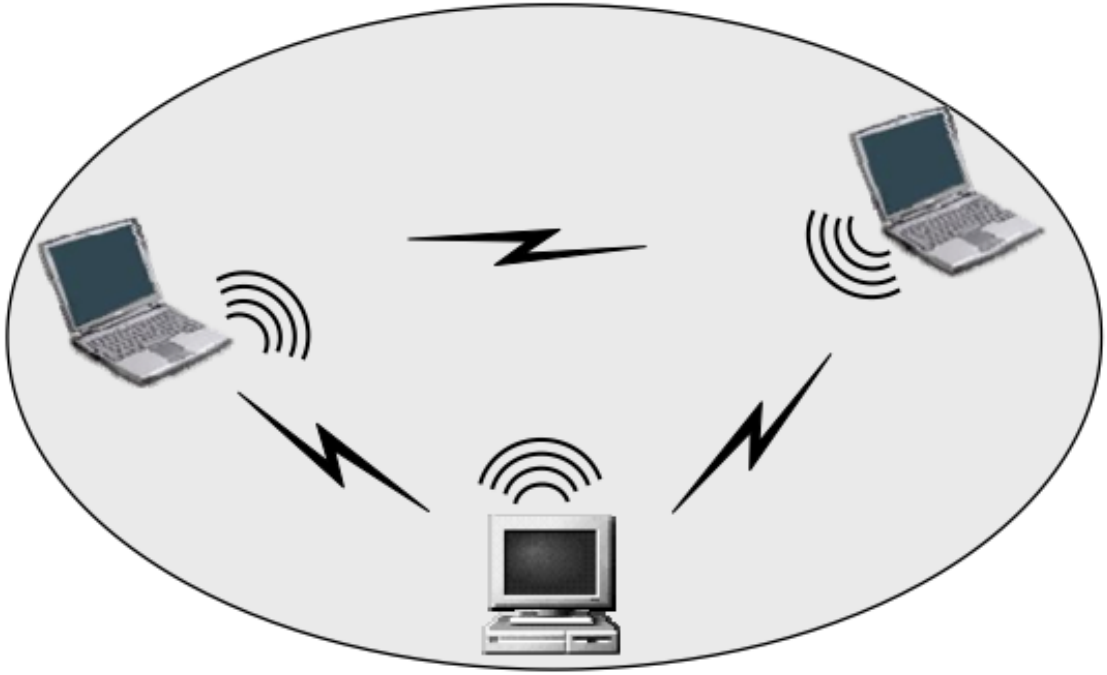
Le réseau Wifi

- La constitution d'un réseau local sans fil se fait selon un mode dit d'infrastructure.
- Le point d'accès est un équipement (antenne émettrice/réceptrice) connecté au réseau filaire Ethernet.
- Chaque ordinateur, équipé lui-même d'une carte WIFI, communique avec ce point d'accès pour pouvoir dialoguer avec les autres machines du réseau.



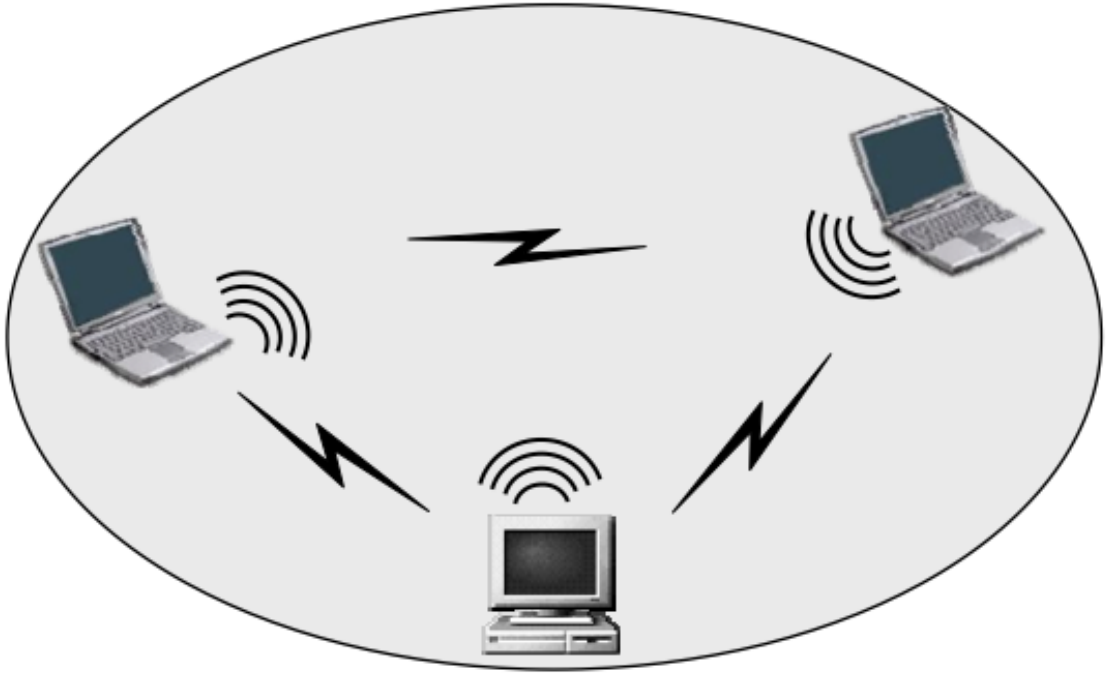
Le réseau Wifi

- La mode ad-hoc consiste à créer un réseau d'ordinateurs équipés de carte WIFI, s'interconnectant entre eux, sans point d'accès particulier ni réseau filaire auquel se raccorder.
- Cela permet de constituer un réseaux de machines sans aucune structure matérielle préexistante.



Le réseau Wifi

- La mode ad-hoc consiste à créer un réseau d'ordinateurs équipés de carte WIFI, s'interconnectant entre eux, sans point d'accès particulier ni réseau filaire auquel se raccorder.
- Cela permet de constituer un réseaux de machines sans aucune structure matérielle préexistante.



Le réseau Wifi

- Les émissions de données sont régies par la technique CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance)
- Lorsqu'une station veut émettre, elle explore le spectre de fréquences.
- Si une activité est détectée, elle attend pendant quelques instants avant de réessayer.
- Si aucune activité n'est détectée, et si cette inactivité dure un temps donné DIFS (Distributed Inter Frame Space), alors la station expédie ses données et attend un message d'acquittement (ACK).
- Si celui-ci n'arrive pas, soit parce que le récepteur a détecté des incohérences, soit parce qu'il a été lui-même perturbé, alors la station émettrice retransmet les données.
- Sinon, lorsque le ACK est reçu, l'émission est terminée.

Le réseau Wifi

- La phase d'écoute préalable peut être inefficace car l'absence d'activité ne signifie pas forcément aucune activité, notamment à proximité du point d'accès.
- En effet, deux stations peuvent ne pas « s'entendre » si elles sont trop éloignées l'une de l'autre, tout en étant chacune à portée du point d'accès.
- Pour pallier cette difficulté, la station émettrice, après avoir constaté une période de silence, va envoyer un message RTS (Ready To Send). Ce message contient des informations sur le volume des données à émettre et la vitesse de transmission.
- Le récepteur répond alors par un message CTS (Clear To Send), puis la station expédie les données.
- Lorsque toutes les données sont reçues, le récepteur envoie un accusé de réception (ACK).
- Grâce au message CTS qui peut être reçu par toutes les stations (car elles sont toutes à portée du point d'accès), ces dernières vont rester silencieuses pendant le temps nécessaire à la transmission des données à la vitesse annoncée.
- Ce mécanisme RTS/CTS, qui évite de créer des collisions, n'est utilisé que pour les « gros » paquets de données.
- Les protocoles 802.11 assurent aussi la fragmentation des paquets de manière à expédier peu de données à la fois ce qui améliore les taux de transfert et chaque paquet est protégé par un CRC de 32 bits.

Le routage IP

- Le routage est l'une des fonctionnalités principales de la couche IP et consiste à choisir la manière de transmettre un datagramme IP à travers les divers réseaux d'un internet.
- On appellera ordinateur un équipement relié à un seul réseau et 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).
- Ainsi un routeur réémettra des datagrammes venus d'une de ses interfaces vers une autre, alors qu'un ordinateur sera soit l'expéditeur initial, soit le destinataire final d'un datagramme.

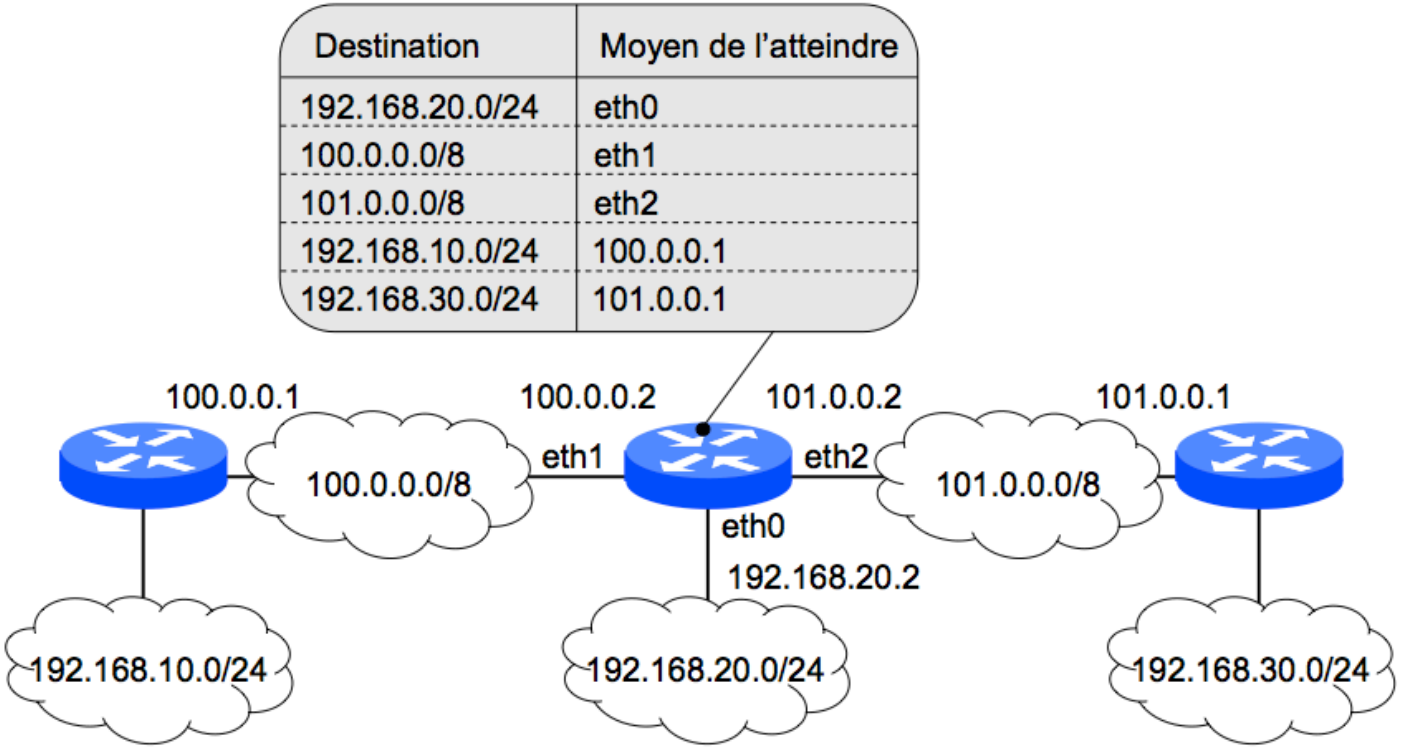
Le routage IP

- D'une manière générale on distingue la **remise directe**, qui correspond au transfert d'un datagramme entre deux ordinateurs du même réseau, et **la remise indirecte** qui est mise en oeuvre dans tous les autres cas, c'est-à-dire quand au moins un routeur sépare l'expéditeur initial et le destinataire final.
- Par exemple, dans le cas d'un réseau Ethernet, la remise directe consiste à encapsuler le datagramme dans une trame Ethernet après avoir utilisé le protocole ARP pour faire la correspondance adresse IP adresse physique et à émettre cette trame sur le réseau.
    - L'expéditeur peut savoir que le destinataire final partage le même réseau que lui-même en utilisant simplement l'adresse IP de destination du datagramme.
    - Il en extrait l'identificateur de réseau et si c'est le même que celui de sa propre adresse IP
    - La remise directe est suffisante.
    - Ce mécanisme de remise directe se retrouve toujours lors de la remise d'un datagramme entre le dernier routeur et le destinataire final.
- La remise indirecte nécessite de 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 qui permet de déterminer vers quelle voie de sortie envoyer un datagramme destiné à un réseau quelconque.
- À cause de la structure localement arborescente d'internet la plupart des tables de routage ne sont pas très grandes. Par contre, les tables des routeurs interconnectant les grands réseaux peuvent atteindre des tailles très grandes ralentissant d'autant le trafic sur ces réseaux.

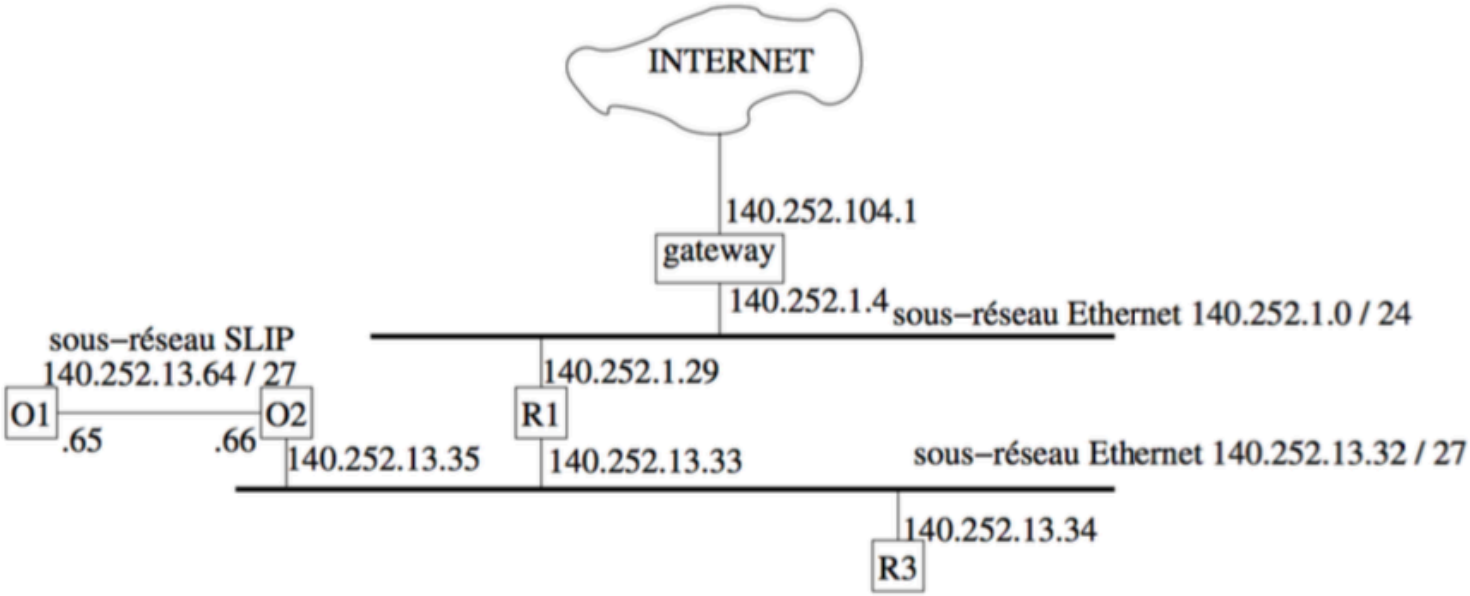
Le routage IP

- L'essentiel du contenu d'une table de routage est constitué de quadruplet (destination, passerelle, masque, interface)} où :
  - destination est l'adresse IP d'une machine ou d'un réseau de destination,
  - passerelle (gateway) est l'adresse IP du prochain routeur vers lequel envoyer le datagramme pour atteindre cette destination,
  - masque est le masque associé au réseau de destination,
  - interface désigne l'interface physique par laquelle le datagramme doit réellement être expédié.
  - Une table de routage contient notamment une route par défaut qui spécifie un routeur vers lequel sont envoyés tous les datagrammes pour lesquels il n'existe pas de route spécifique dans la table.
  - Tous les routeurs mentionnés dans une table de routage doivent bien sûr être directement accessibles à partir du routeur considéré.
  - Cette technique, dans laquelle un routeur ne connaît pas le chemin complet menant à une destination, mais simplement la première étape de ce chemin, est appelée routage par sauts successifs (next-hop routing).

Le routage IP



Le routage IP



destination	gateway	genmask	flags	refcnt	use	interface
140.252.13.65	140.252.13.35	255.255.255.255	UGH	0	0	emd0
127.0.0.1	127.0.0.1	255.255.255.255	UH	1	0	lo0
140.252.13.32	140.252.13.34	255.255.255.254	U	4	25043	emd0
default	140.252.13.33	0.0.0.0	UG	0	0	emd0

Le routage IP

- Les flags ont la signification suivante :
  - U : La route est en service.
  - G : La route est un routeur (gateway). Si ce flag n'est pas positionné la destination est directement connectée au routeur, c'est donc un cas de remise directe vers l'adresse IP de destination.
  - H : La route est un ordinateur (host), la destination est une adresse d'ordinateur. Dans ce cas, la correspondance entre l'adresse de destination du paquet à « router » et l'entrée destination de la table de routage doit être totale. Si ce flag n'est pas positionné, la route désigne un autre réseau et la destination est une adresse de réseau ou de sous-réseau. Ici, la correspondance des identificateurs de réseaux est suffisante.
  - D : La route a été créée par une redirection.
  - M : La route a été modifiée par une redirection.
- La colonne compteur de référence (refcnt) indique le nombre de fois où la route est utilisée à l'instant de la consultation.
- La colonne use affiche le nombre de paquets envoyés à travers l'interface de cette route qui est spécifiée dans la dernière colonne de la même ligne.
- L'adresse 127.0.0.1 est celle de lo0 l'interface de loopback, qui sert à pouvoir faire communiquer une machine avec elle-même.
- La destination default sert à indiquer la destination de tous les datagrammes qui ne peuvent être « routés » par l'une des autres routes. Elle est placée en dernière position, puisque la décision de routage se fait selon l'ordre des lignes de la table.
- La première entrée (ligne) dont l'adresse de destination est égale à l'adresse de destination du paquet à router « modulo le masque » indique l'interface de sortie par laquelle expédier ce paquet.

Le routage IP

- L'établissement d'une table de routage est :
  - Statique lorsqu'elle résulte de la configuration par défaut d'une interface, ou de la commande *route* à partir d'un fichier de démarrage, ou grâce à une redirection ICMP.
  - Dès que le réseau devient non trivial, on utilise le routage dynamique qui consiste en un protocole de communication entre routeurs qui informent chacun de leurs voisins des réseaux auxquels ils sont connectés. Grâce à ce protocole, les tables de routage évoluent dans le temps en fonction de l'évolution des routes.

Routing Information Protocol

- L'un des protocoles de routage qui fut parmi les plus utilisés est RIP (Routing Information Protocol)
- RIP est un protocole de type vecteur de distance : les messages échangés par des routeurs voisins contiennent un ensemble de distances entre routeur et destinations qui permet de réactualiser les tables de routage.
- Ce protocole utilise une métrique simple : la distance entre une source et une destination est égale au nombre de sauts qui les séparent. Elle est comprise entre 1 et 15, la valeur 16 représentant l'«infini». Ceci implique que RIP ne peut être utilisé qu'à l'intérieur de réseaux qui ne sont pas trop étendus.

Routing Information Protocol

- À l'initialisation, le démon de routage envoie une requête RIP à chaque interface pour demander les tables de routage complètes de chacun de ses voisins.
- Sur une liaison point à point la requête est envoyée à l'autre extrémité, sinon elle est envoyée sous forme de broadcast sur un réseau.
- Le fonctionnement normal de RIP consiste à diffuser des annonces soit toutes les 30 secondes, soit pour une mise à jour déclenchée par la modification de la métrique d'une route.
- Ces annonces sont diffusées par les routeurs à chacun de leurs voisins. Une annonce contient une adresse de destination, accompagnée de sa métrique, de l'adresse du prochain routeur, d'un indicateur de mise à jour récente et de temporisations.
- Le processus RIP met à jour sa table de routage locale en examinant les entrées retournées dont il vérifie d'abord la validité puis il effectue ensuite les mises à jour propres à l'algorithme vecteur de distance suivant :
    - Si l'entrée n'existait pas dans la table et si la métrique reçue n'est pas infinie, alors on ajoute cette nouvelle entrée composée de la destination, de l'adresse du prochain routeur (c'est celui qui envoie la réponse), de la métrique reçue. On initialise la temporisation correspondante.
    - Si l'entrée était présente avec une métrique supérieure à celle reçue, on met à jour la métrique et le prochain routeur et on réinitialise la temporisation.
    - Si l'entrée était présente et que le routeur suivant correspond à l'émetteur de la réponse, on réinitialise la temporisation et on met à jour la métrique avec celle reçue si elles diffèrent.
    - Dans les autres cas on ignore l'entrée.

Open Shortest Path First

- À OSPF (Open Shortest Path First) est un protocole de routage dynamique :
  - Elimine certaines limitations de RIP
  - L'un des plus usités comme protocole de routage interne.
  - C'est un protocole d'état de liens
    - Un routeur n'envoie pas des distances à ses voisins, mais il teste l'état de la connectivité qui le relie à chacun de ses voisins.
    - Il envoie cette information à tous ses voisins, qui ensuite le propagent dans le réseau.
    - Ainsi, chaque routeur peut posséder une carte de la topologie du réseau qui se met à jour très rapidement.
    - Cette carte est un graphe orienté où les arcs sont affectés d'un coût (distance, délai de transmission, etc.), qui permet de calculer des routes aussi précises qu'avec un algorithme centralisé.

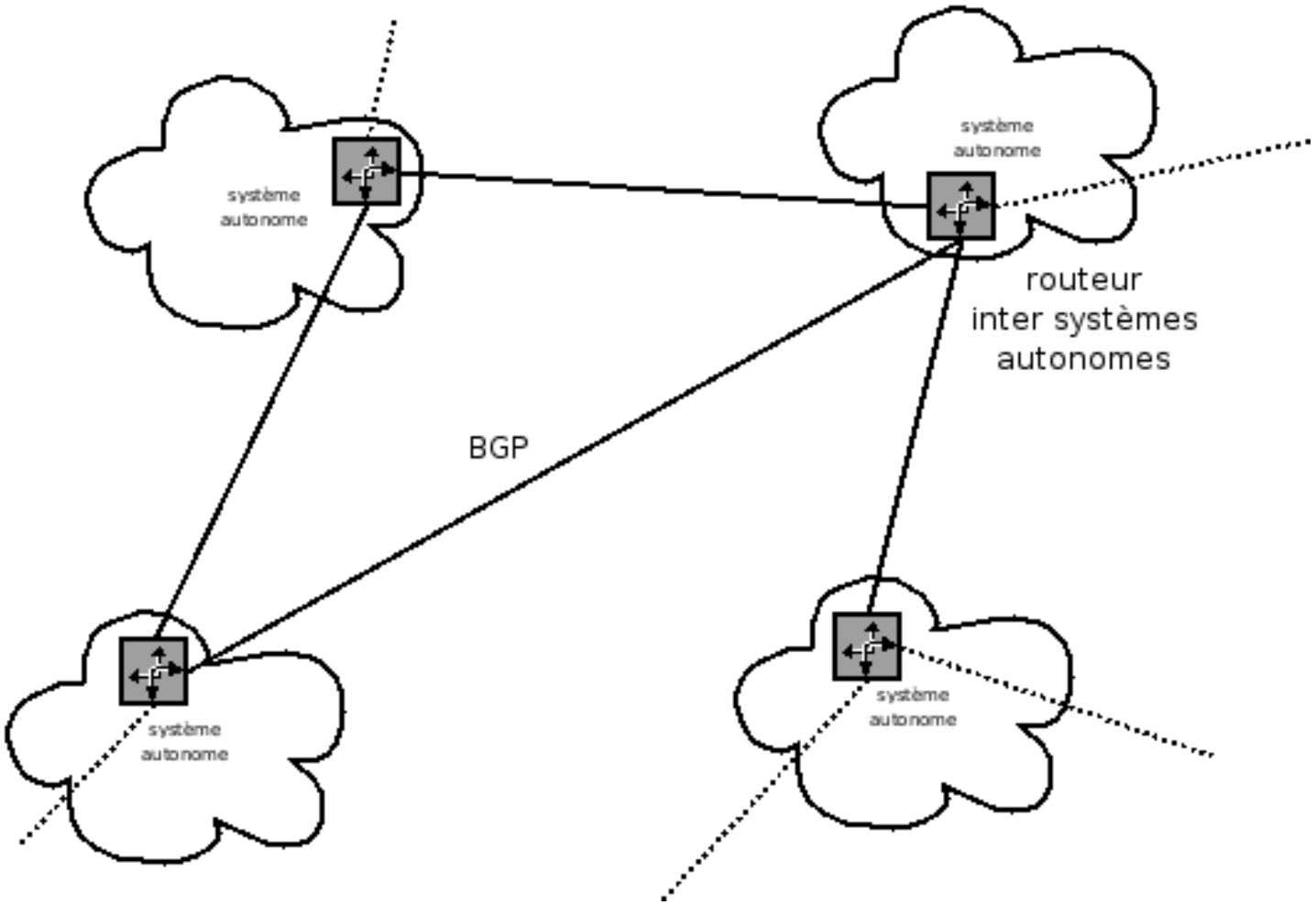
IGP/BGP

- ROP et OSPF sont des protocoles de type IGP (Interior Gateway Protocol) permettant d'établir les tables des routeurs internes des systèmes autonomes.
- Un système autonome peut être défini par un ensemble de routeurs et de réseaux sous une administration unique.
- La règle de base étant qu'un système autonome assure la connexité totale de tous les points qui le composent en utilisant notamment un protocole de routage interne unique (a priori OSPF)
- Dans chaque système autonome les tables de routage sont maintenues par un IGP et sont échangées uniquement entre routeurs du même sous-système.

IGP/BGP

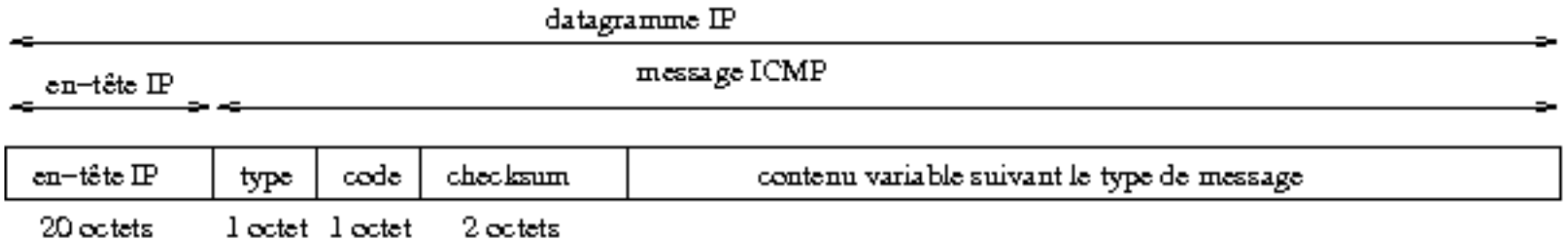
- Pour obtenir des informations sur les réseaux externes, ceux d'un autre système autonome, ils doivent dialoguer avec les routeurs externes de frontière.
- Ceux-ci sont des points d'entrée de chaque système et, via la liaison qui les relie, ils échangent des informations sur la connectivité grâce au protocole BGP (Border Gateway Protocol).
- La particularité de BGP est d'établir des tables de routage en fonction d'accords commerciaux, de considération politiques ou de sécurité, par exemple, et non en fonction d'un plus court chemin.

IGP/BGP


système
autonome
système
autonome
routeur
inter systèmes
autonomes
BGP
système
autonome
système
autonome

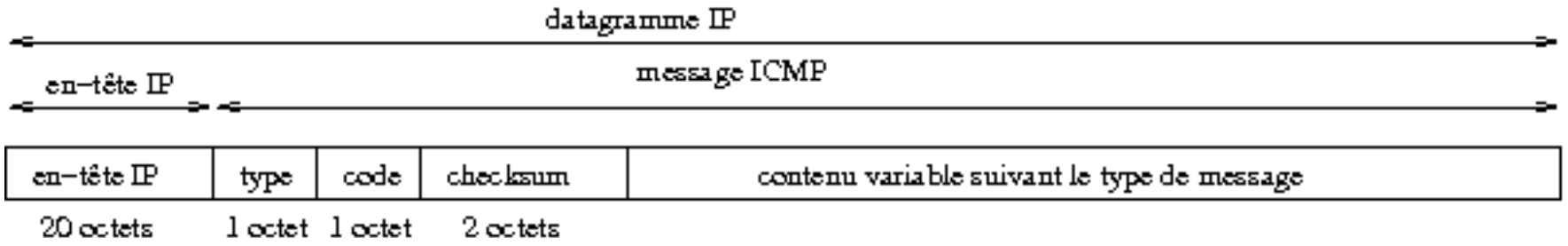
ICMP : La gestion des erreurs

- Le protocole ICMP (Internet Control Message Protocol) organise un échange d'information permettant aux routeurs d'envoyer des messages d'erreurs à d'autres ordinateurs ou routeurs.
- Bien qu'ICMP « tourne » au-dessus de IP il est requis dans tous les routeurs c'est pourquoi on le place dans la couche IP.
- Le but d'ICMP n'est pas de rendre fiable le protocole IP, mais de fournir à une autre couche IP, ou à une couche supérieure de protocole (TCP ou UDP), le compte-rendu d'une erreur détectée dans un routeur.
- Un message ICMP étant acheminé à l'intérieur d'un datagramme IP, il est susceptible, lui aussi, de souffrir d'erreurs de transmission.



ICMP : La gestion des erreurs

- Le champ type peut prendre 15 valeurs différentes spécifiant de quelle nature est le message envoyé.
- Pour certains types, le champ code sert à préciser encore plus le contexte d'émission du message.
- Le checksum est une somme de contrôle de tout le message ICMP calculée comme dans le cas de l'en-tête d'un datagramme IP.
- Des exemples des différentes catégories de messages sont donnés dans la liste ci-dessous où chaque alinéa commence par le couple (type, code) de la catégorie décrite :



ICMP : La gestion des erreurs

- (0,0) ou (8,0) : Demande (type 8) ou réponse (type 0) d'écho dans le cadre de la commande ping.
- (3,0-13) : Compte-rendu de destination inaccessible délivré quand un routeur ne peut délivrer un datagramme.
  - 0 Le réseau est inaccessible.
  - 1 La machine est inaccessible.
  - 2 Le protocole est inaccessible.
  - …
- (4,0) Demande de limitation de production pour éviter la congestion du routeur qui envoie ce message.
- (5,0-3) Demande de modification de route expédiée lorsqu'un routeur détecte qu'un ordinateur utilise une route non optimale
  - 0 Redirection pour un réseau.
  - 1 Redirection pour une machine.
  - 2 Redirection pour un type de service et réseau.
  - 3 Redirection pour un type de service et machine.

ICMP : La gestion des erreurs

- (9,0) Avertissement de routeur expédié par un routeur.
- (10,0) Sollicitation de routeur diffusé par une machine pour initialiser sa table de routage.
- (11,0) TTL détecté à 0 pendant le transit du datagramme IP, lorsqu'il y a une route circulaire ou lors de l'utilisation de la commande traceroute.
- (11,1) TTL détecté à 0 pendant le réassemblage d'un datagramme.
- (12,0) Mauvaise en-tête IP.
- (12,1) Option requise manquante.
- (13-14,0) Requête (13) ou réponse (14) timestamp, d'estampillage horaire.
- (15,0) et (16,0) devenues obsolètes.
- (17-18,0) Requête (17) ou réponse (18) de masque de sous-réseau.

Le protocole UDP

- Le protocole UDP (User Datagram Protocol, RFC 768) utilise IP pour acheminer, d'un ordinateur à un autre, en mode non fiable des datagrammes qui lui sont transmis par une application.
- UDP n'utilise pas d'accusé de réception et ne peut donc pas garantir que les données ont bien été reçues.
- UDP ne réordonne pas les messages si ceux-ci n'arrivent pas dans l'ordre dans lequel ils ont été émis et il n'assure pas non plus de contrôle de flux.
- Il se peut donc que le récepteur ne soit pas apte à faire face au flux de datagrammes qui lui arrivent.
- C'est donc à l'application qui utilise UDP de gérer les problèmes de perte de messages, duplications, retards, déséquencement, etc.

Le protocole UDP

- Le protocole UDP (User Datagram Protocol, RFC 768) utilise IP pour acheminer, d'un ordinateur à un autre, en mode non fiable des datagrammes qui lui sont transmis par une application.
- UDP n'utilise pas d'accusé de réception et ne peut donc pas garantir que les données ont bien été reçues.
- UDP ne réordonne pas les messages si ceux-ci n'arrivent pas dans l'ordre dans lequel ils ont été émis et il n'assure pas non plus de contrôle de flux.
- Il se peut donc que le récepteur ne soit pas apte à faire face au flux de datagrammes qui lui arrivent.
- C'est donc à l'application qui utilise UDP de gérer les problèmes de perte de messages, duplications, retards, déséquencement, etc.

Le protocole UDP

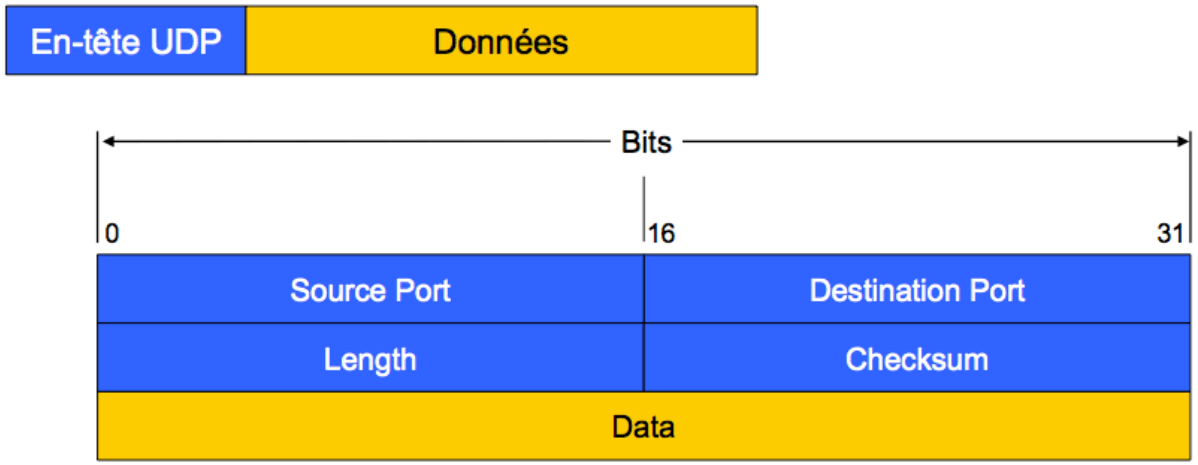
- UDP fournit un service supplémentaire par rapport à IP : il permet de distinguer plusieurs applications destinataires sur la même machine par l'intermédiaire des ports.
- Un port est une destination abstraite sur une machine identifié par un numéro qui sert d'interface à l'application pour recevoir et émettre des données.
- Par exemple :

```
discard    9/udp    sink null
systat     11/udp   users
daytime    13/udp
```

est un court extrait d'un fichier */etc/services* dans lequel sont enregistrés les numéros de port utilisés par chaque application.

Le protocole UDP

- Chaque datagramme émis par UDP est encapsulé dans un datagramme IP en y fixant à 17 la valeur du protocole
- Le format d'un d'anagramme UDP est le suivant :
  - Les numéros de port (chacun sur 16 bits) identifient les processus émetteur et récepteur.
  - Le champ longueur contient sur 2 octets la taille de l'en-tête et des données transmises. Puisqu'un datagramme UDP peut ne transmettre aucune donnée la valeur minimale de la longueur est 8.
  - Le checksum est un total de contrôle qui est optionnel car il n'est pas indispensable lorsque UDP est utilisé sur un réseau très fiable. S'il est fixé à 0 c'est qu'en fait il n'a pas été calculé.



Le protocole TCP

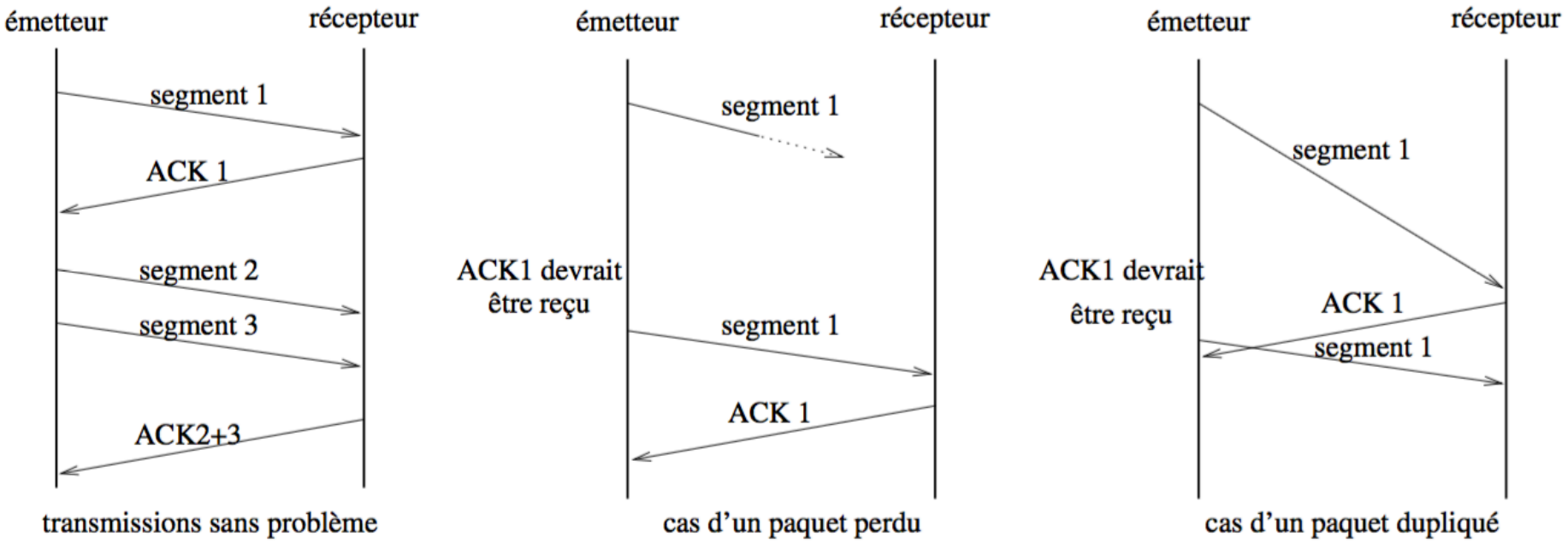
- Contrairement à UDP, TCP (Transmission Control Protocol) est un protocole qui procure un service de flux d'octets **orienté connexion** et **fiable**.
- Les données transmises par TCP sont encapsulées dans des datagrammes IP en y fixant la valeur du protocole à 6.
- Une connexion TCP est bidirectionnelle simultanée full duplex et composée de deux flots de données indépendants et de sens contraire.

Le protocole TCP

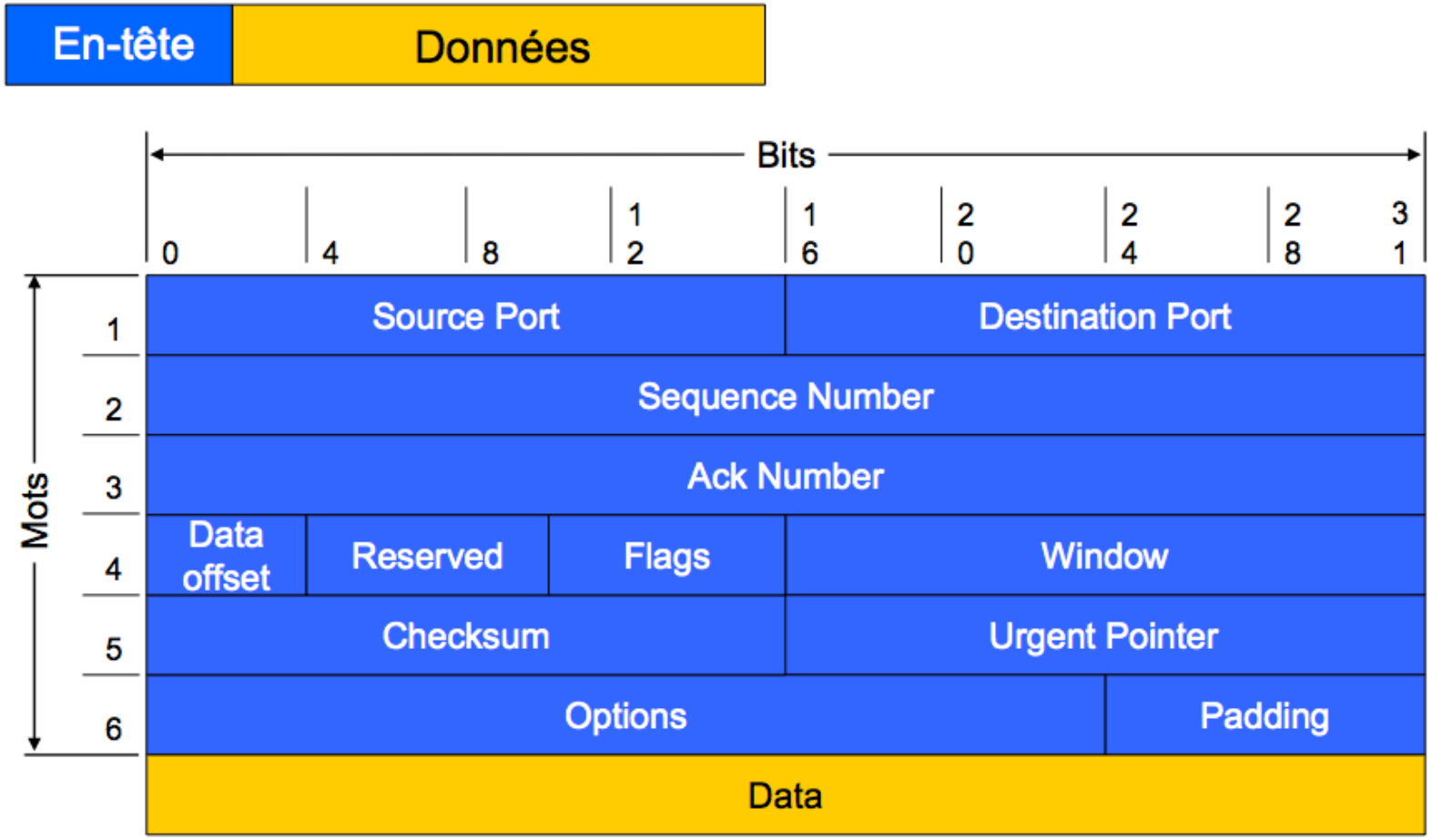
- Contrairement à UDP, TCP (Transmission Control Protocol) est un protocole qui procure un service de flux d'octets **orienté connexion** et **fiable**.
- Les données transmises par TCP sont encapsulées dans des datagrammes IP en y fixant la valeur du protocole à 6.
- Une connexion TCP est bidirectionnelle simultanée full duplex et composée de deux flots de données indépendants et de sens contraire.
- Des segments TCP sont envoyés d'une extrémité à une autre

Acquittement dans TCP

- La fiabilité fournie par TCP consiste à remettre des datagrammes, sans perte, ni duplication
- Ceci est réalisé à l'aide de la technique générale de l'accusé de réception (ACK) présentée ci-dessous de manière simplifiée



Segment TCP


En-tête
Données
Bits
0
4
8
12
16
20
24
28
31
Mots
1
2
3
4
5
6
Source Port
Destination Port
Sequence Number
Ack Number
Data offset
Reserved
Flags
Window
Checksum
Urgent Pointer
Options
Padding
Data

Segment TCP

- Le port source et le port destination identifient les applications émettrice et réceptrice. En les associant avec les numéros IP source et destination du datagramme IP qui transporte un segment TCP on identifie de manière unique chaque connexion
- Le numéro de séquence donne la position du segment dans le flux de données envoyées par l'émetteur; c'est-à-dire la place dans ce flux du premier octet de données transmis dans ce segment.
- Le numéro d'accusé de réception contient en fait le numéro de séquence suivant que le récepteur s'attend à recevoir; c'est-à-dire le numéro de séquence du dernier octet reçu avec succès plus 1. De manière précise, TCP n'acquitte pas un à un chaque segment qu'il reçoit, mais acquitte l'ensemble du flot de données jusqu'à l'octet en envoyant un acquittement de valeur .
  - Par exemple, dans une transmission de 3 segments de A vers B, si les octets de 1 à 1024 sont reçus correctement, alors B envoie un ACK avec la valeur 1025.
  - Puis, si le segment suivant contenant les octets de 1025 à 2048 se perd et que B reçoit d'abord correctement le segment des octets de 2049 à 3072, B n'enverra pas d'accusé de réception positif pour ce troisième segment.
  - Ce n'est que lorsque B recevra le deuxième segment, qu'il pourra envoyer un ACK avec la valeur 3073, que A interprétera comme l'acquittement des deux derniers segments qu'il a envoyés. On appelle cela un acquittement cumulatif.

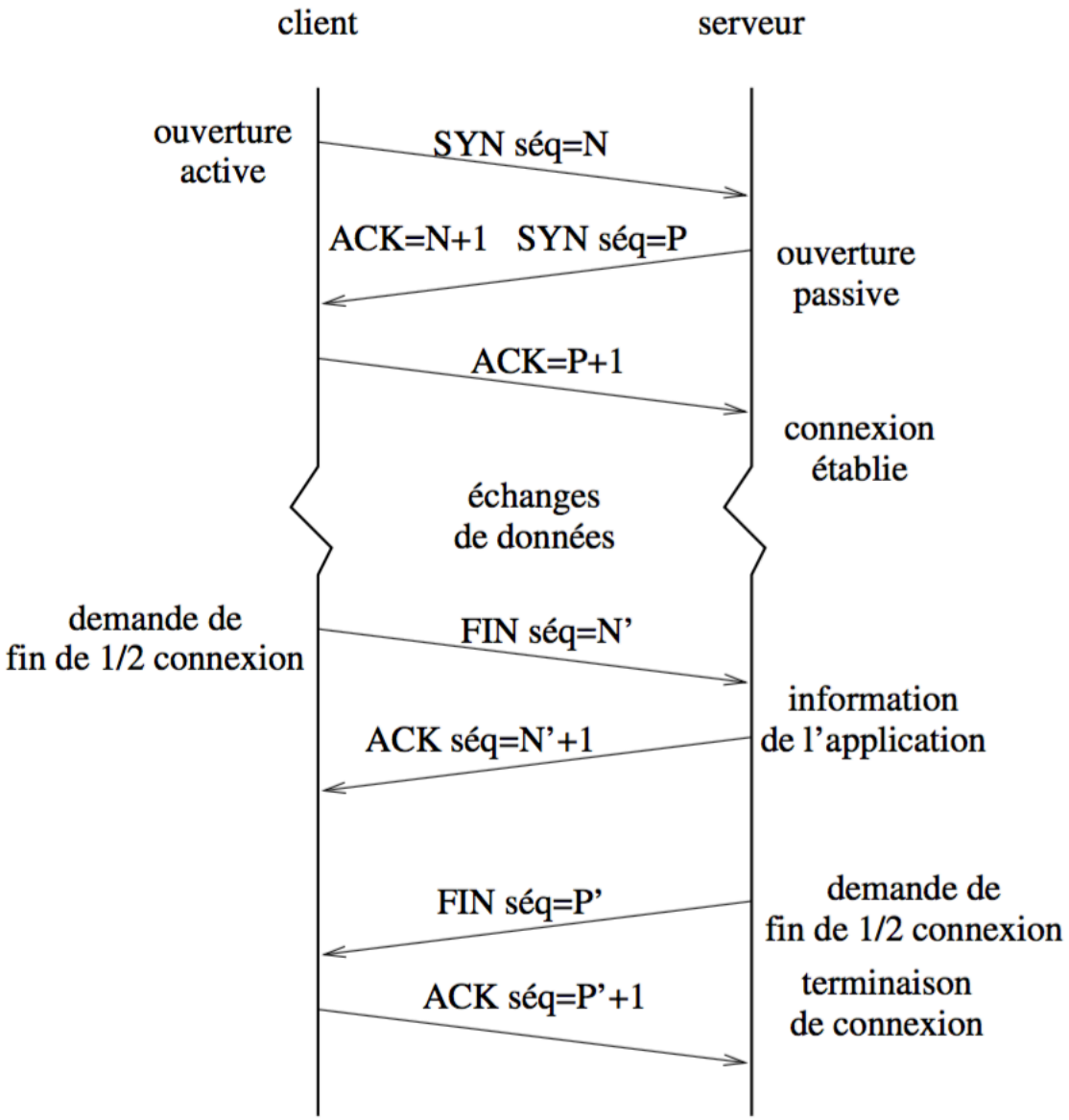
Segment TCP

- La longueur d'en-tête contient sur 4 bits la taille de l'en-tête, y compris les options présentes, codée en multiple de 4 octets. Ainsi une en-tête peut avoir une taille variant de 20 octets (aucune option) à 60 octets (maximum d'options).
- Le champ réservé comporte 6 bits réservés à un usage ultérieur.
- Les 6 champs bits de code qui suivent permettent de spécifier le rôle et le contenu du segment TCP pour pouvoir interpréter correctement certains champs de l'en-tête. La signification de chaque bit, quand il est fixé à 1 est la suivante :
  - URG, le pointeur de données urgentes est valide.
  - ACK, le champ d'accusé de réception est valide.
  - PSH, ce segment requiert un push.
  - RST, réinitialiser la connexion.
  - SYN, synchroniser les numéros de séquence pour initialiser une connexion.
  - FIN, l'émetteur a atteint la fin de son flot de données.

Segment TCP

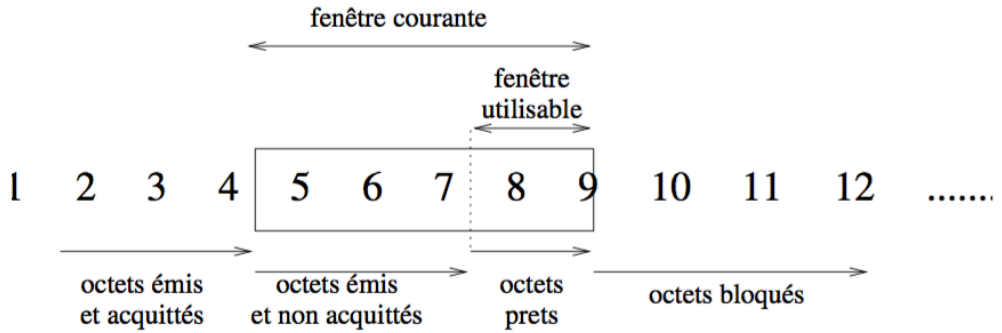
- La taille de fenêtre est un champ de 16 bits qui sert au contrôle de flux selon la méthode de la fenêtre glissante. Il indique le nombre d'octets (moins de 65535) que le récepteur est prêt à accepter. Ainsi l'émetteur augmente ou diminue son flux de données en fonction de la valeur de cette fenêtre qu'il reçoit.
- Le checksum est un total de contrôle sur 16 bits utilisé pour vérifier la validité de l'en-tête et des données transmises.
- Le pointeur d'urgence est un offset positif qui, ajouté au numéro de séquence du segment, indique le numéro du dernier octet de donnée urgente. Il faut également que le bit URG soit positionné à 1 pour indiquer des données urgentes que le récepteur TCP doit passer le plus rapidement possible à l'application associée à la connexion.
- L'option la plus couramment utilisée est celle de la taille maximale du segment TCP qu'une extrémité de la connexion souhaite recevoir.

Connexion et déconnexion TCP

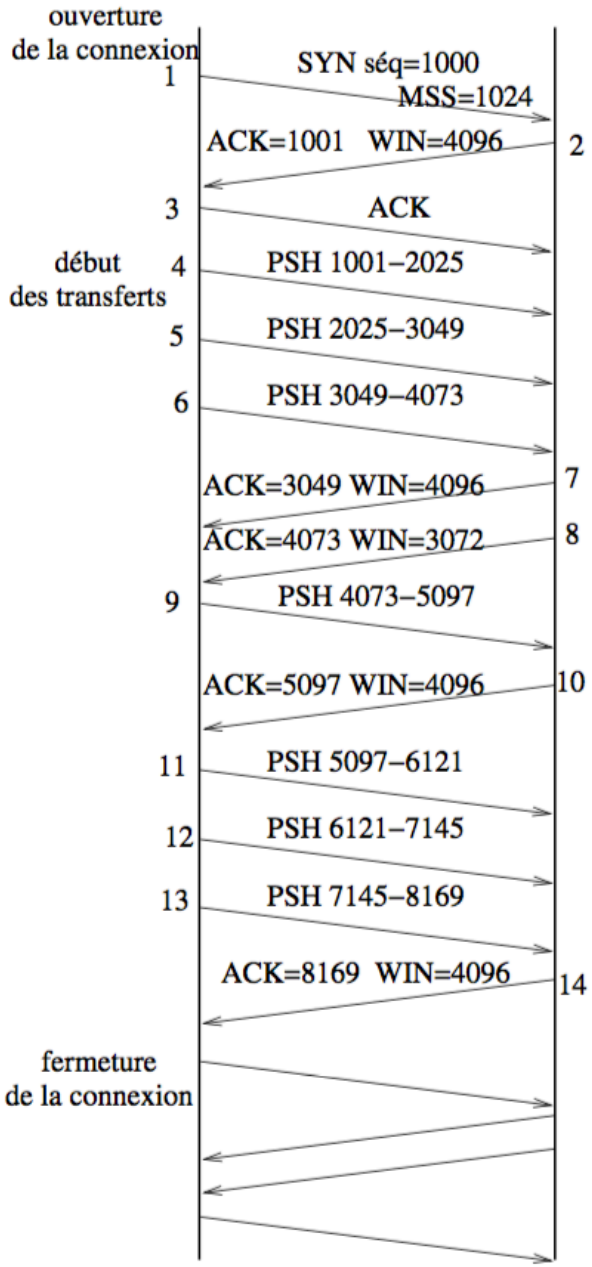


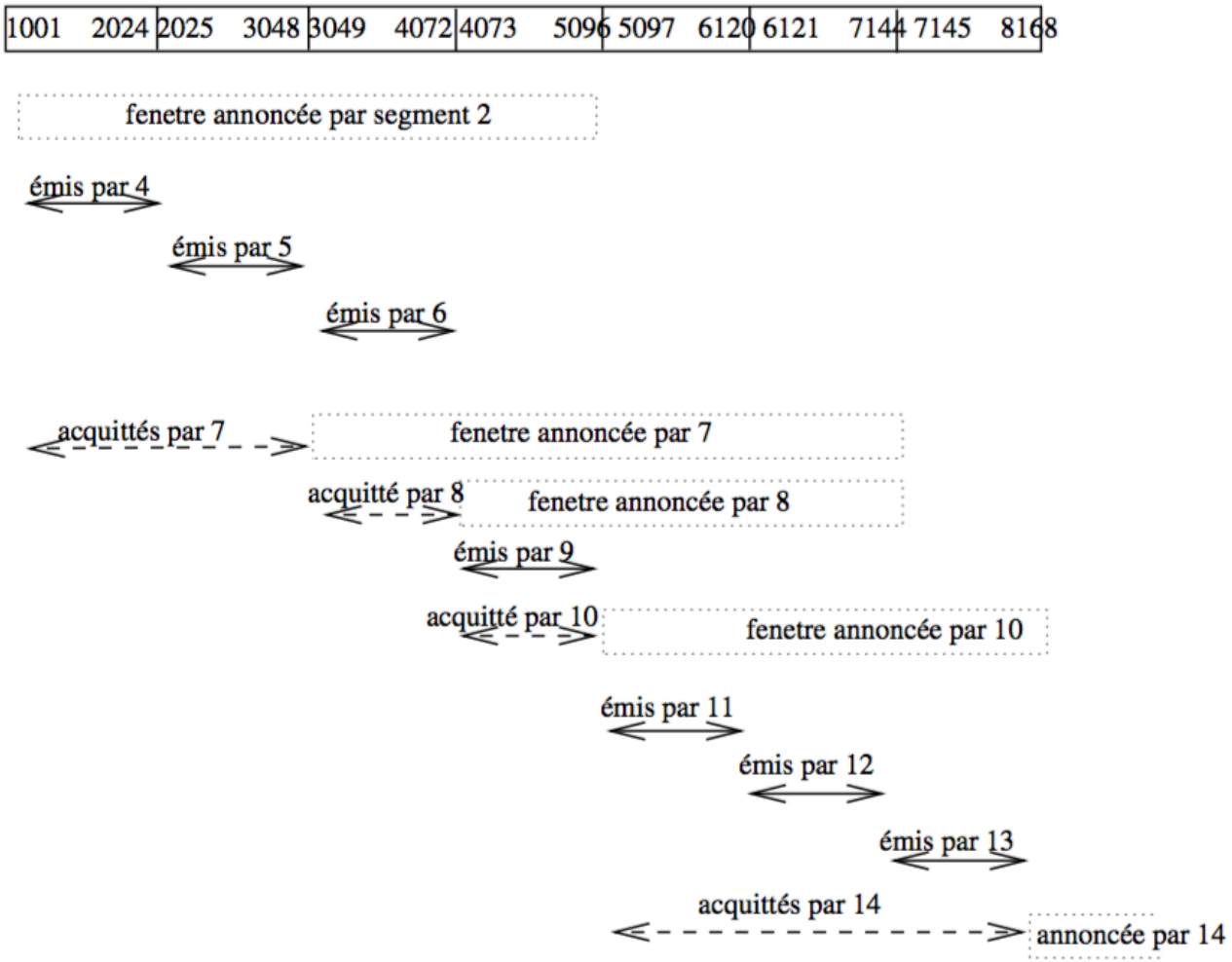
Contrôle des flux

- TCP utilise la technique de la fenêtre glissante pour contrôler le flux des échanges.
- L'ensemble d'un flux de données unidirectionnel d'une machine A vers une machine B est constitué d'une séquence d'octets tous numérotés individuellement.
- A tout instant TCP calcule sa fenêtre utilisable qui est constituée des octets présents dans la fenêtre et non encore envoyés. Ces octets sont généralement immédiatement transmis.
- Pour le flot de A vers B, la taille de la fenêtre est contrôlée par B qui envoie dans chacun de ses accusés de réception la taille de la fenêtre qu'il désire voir utiliser.
- Si la demande exprime une augmentation, A déplace le bord droit de sa fenêtre courante et émet immédiatement les octets qui viennent d'y entrer.
- Si la demande exprime une diminution, il est déconseillé de déplacer réellement le bord droit de la fenêtre vers la gauche. Ce rétrécissement est opéré lors des glissements de la fenêtre vers la droite avec l'arrivée des accusés de réception.



Contrôle des flux





Fin de l'épisode