Réseaux

Chapitre 2 - Open Systems Interconnection (OSI)

Claude Duvallet

Université du Havre
UFR Sciences et Techniques
25 rue Philippe Lebon - BP 540
76058 LE HAVRE CEDEX
Claude.Duvallet@gmail.com

Plan de la présentation

Couche physique (niveau 1)

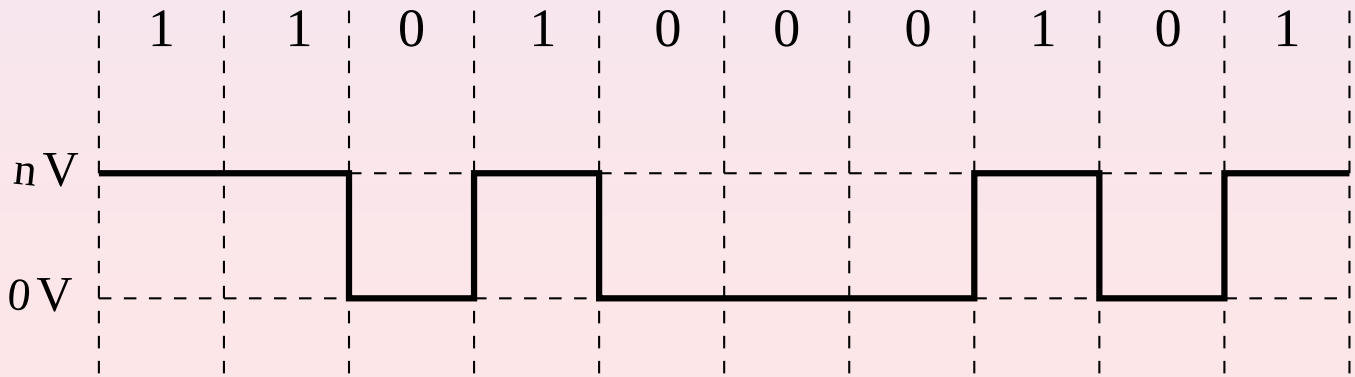
- Transmission de données binaires au niveau matériel.
- Supports de transmission très variés :
  - câbles électriques, fibres optiques, câble Ethernet, câble coaxiale,
  - liaison radio, laser, etc.
- Techniques de transmission binaire propres à chacun de ces supports :
  - définition du temps nécessaire pour qu'un bit soit diffusé,
  - ergonomie d'un connecteur ou standard de brochage dans ces connecteurs.
- Capacité à autoriser une communication bidirectionnelle ou plusieurs communications sur une même ligne physique unique.

Les modes d'exploitation

- Il existe trois modes d'exploitation d'une ligne de transmission :
  - Les communications simplex entre deux équipements n'autorisent le passage que dans un seul sens. L'émetteur et le récepteur sont alors deux entités distinctes et c'est l'émetteur qui dirige la transmission.
  - Les communications semi-duplex (half duplex) permettent à des données de transiter dans les deux sens sur un support physique unique, mais non simultanément. Le premier émetteur est l'initiateur de la communication.
  - Les communications duplex (full-duplex) permettent de mettre en place sur une ligne des transferts bidirectionnels simultanés. Dans ce cas, plusieurs techniques de multiplexage peuvent être utilisées.

Transmission en bande de passe (1/6)

- Description :
  - réseaux locaux $\Rightarrow$ distance entre deux ordinateurs faible.
  - le signal émis sur un câble électrique reste donc peu affaibli.
  - transmission en bande de passe : les données binaires codées par un signal numérique sont transmises directement sur le câble.
  - le codage le plus simple consiste à faire correspondre au bit 1 un signal électrique de tension *n* volts et au bit 0 un signal de tension nulle.
  - exemple : transmission de la valeur 1101000101.



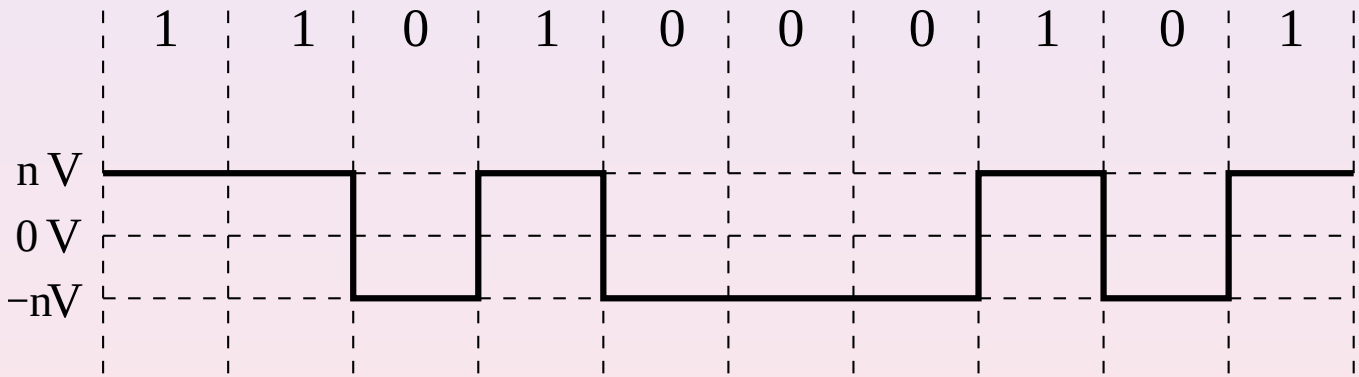
Transmission en bande de passe (2/6)

- Problèmes posés par le codage trop simple :
  - une tension nulle correspond à l'envoi d'un 0 binaire mais peut aussi correspondre à l'absence d'envoi de données.
  - si une suite binaire comprend plusieurs 0 ou 1 binaires consécutifs, il faut que l'émetteur et le récepteur soient parfaitement synchronisés pour que le décodage se fasse correctement.

  $\Rightarrow$ cela peut conduire le récepteur à ne pas reconnaître les données reçues.
- Pour éliminer ces problèmes, plusieurs codes plus évolués ont été élaborés :
  - le NRZ pour sa simplicité de conception,
  - le code de Manchester pour sa mise en œuvre dans les réseaux Ethernet,
  - le code de Manchester différentiel,
  - le code de Miller.

Transmission en bande de passe (3/6)

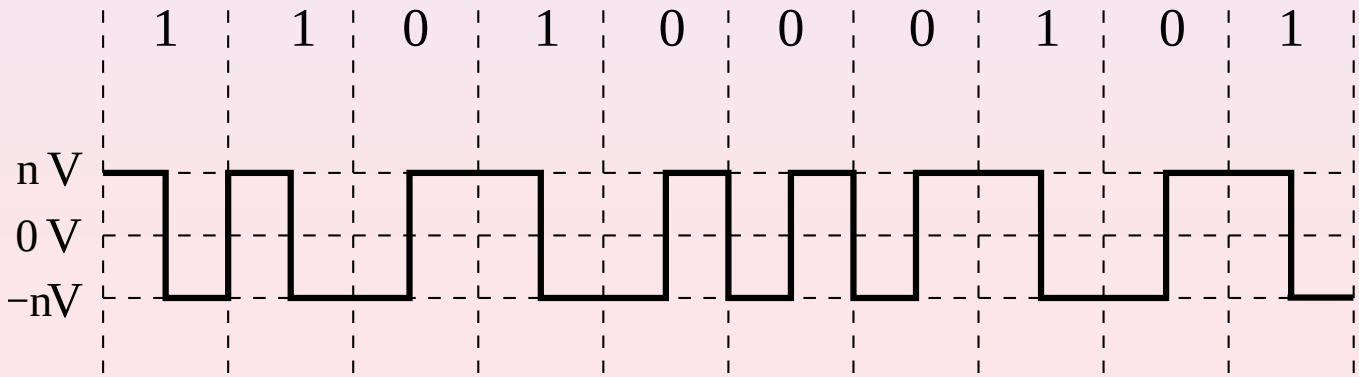
- Le code NRZ (*No Return to Zero*) :
  - résolution du problème d'absence de signal sur le câble,
  - on code le bit 1 par un signal de *n* volts et le bit 0 par un signal opposé.



  - Le code NRZI (*No Return to Zero Inverted*) est similaire au code NRZ mais les tensions associées aux valeurs binaires sont inversées : 1 est codé par une tension négative et 0 par une tension positive.

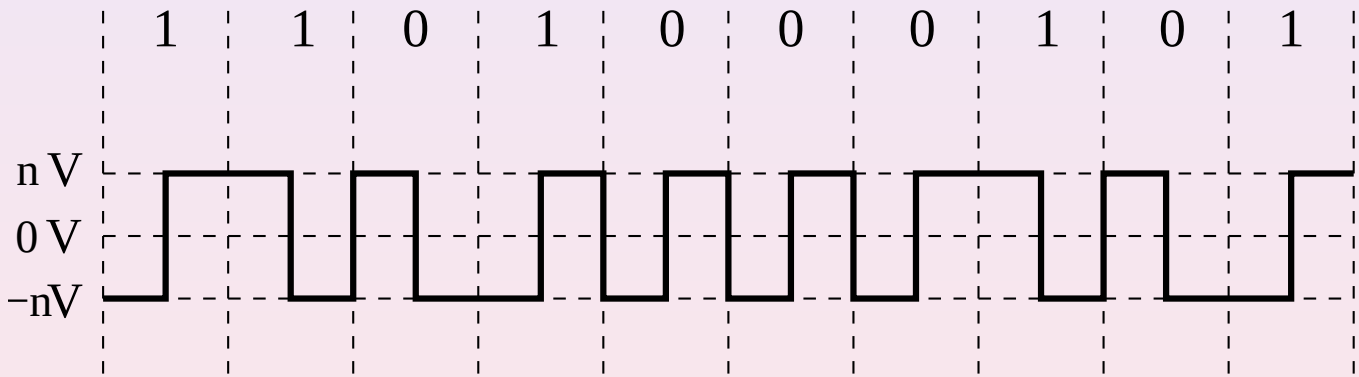
Transmission en bande de passe (4/6)

- Le code Manchester :
  - Il est aussi appelé le code biphase.
  - Il propose une solution au problème de détection des longues chaînes de 0 ou 1.
  - Il s'agit d'un code basé sur les variations du signal : ce n'est plus la tension qui est importante mais la différence de signal.
  - 1 est codé par un passage de la tension *n* à *-n* et 0 par le passage en sens inverse.



Transmission en bande de passe (5/6)

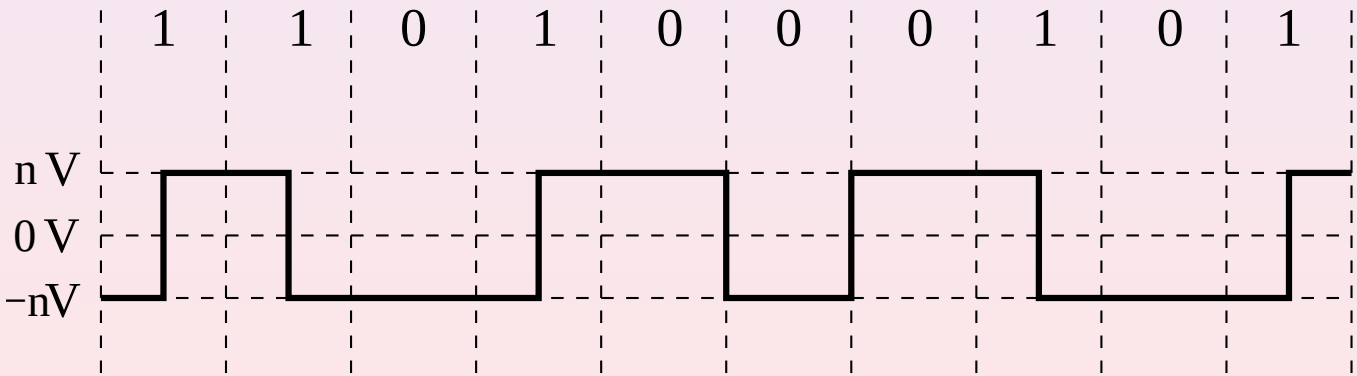
- Le code Manchester différentiel :
  - Il est aussi appelé le code biphase différentiel.
  - Il est similaire au précédent mais le bit 0 est codé par une transition en début d'horloge contrairement au bit 1.



  - Dans les deux cas, un changement de tension est réalisé en milieu de temps horloge.
  - Il a été utilisé dans la norme 802.5 (réseau de type anneau à jeton).

Transmission en bande de passe (6/6)

- Le code Miller :
  - Le bit 1 est codé par une transition en milieu de temps horloge et le bit 0 par une absence de transition.
  - Les longues suites de 0 posant toujours le problème de la synchronisation, si un bit 0 est suivi d'un autre 0 une transition est rajoutée à la fin du temps horloge.



Les supports de transmission (1/12)

- Il existe différents supports de transmission des données sur le marché, les principaux que l'on trouve actuellement sont :
  - les câbles électriques : câbles à paires torsadées et câbles coaxiaux,
  - la fibre optique,
  - l'espace hertzien pour les réseaux sans fil.
- Le câble électrique à paires torsadées :
  - Il est actuellement le support physique le plus répandu.
  - Il est utilisé dans plusieurs cas :
    - connexion d'un poste au concentrateur du réseau (hub, switch,...).
    - interconnexion d'éléments actifs de natures diverses (concentrateurs, commutateurs, relanceurs...).
  - La structure de ce type de câbles est simple : il est constitué de plusieurs fils de cuivre torsadés par paires, ces paires étant à leur tour torsadées entre elles.

Les supports de transmission (2/12)

- Le câble électrique à paires torsadées (suite) :
  - Un câble peut regrouper, suivant les utilisations qui en sont faites, d'une à plusieurs centaines de paires torsadées.
  - Dans le cadre des réseaux locaux, le type le plus commun est de quatre paires torsadées.
  - On peut distinguer différents niveaux de qualité :
    - le câble non blindé, UTP (Unshielded Twisted Pair), support le plus simple et donc le moins coûteux.
    - le câble avec écran : UTP avec écran ou FTP (Foiled Twisted Pairs). L'écran est une simple feuille d'aluminium placée entre les fils et la gaine PVC.
    - le câble blindé, STP (Shielded Twisted Pair), protégé des parasites par une tresse métallique.
    - le câble blindé, SFTP (Shielded Foiled Twisted Pairs), possède à la fois la feuille de blindage en aluminium et la tresse métallique.

Les supports de transmission (3/12)

- Le câble électrique à paires torsadées (suite) :
  - Les connecteurs appropriés à ce type de câbles sont les connecteurs RJ45 pour les 4 paires ou RJ11 pour deux paires.
  - Différentes catégories de câbles ont été définies en fonction de leurs performances :
    - Elles sont nommées Catégorie 1 à Catégorie 5.
    - Une Catégorie 5 améliorée a été créée pour mettre en œuvre les réseaux ATM.
    - Deux autres catégories (Catégorie 6 et Catégorie 7) ont été créées pour permettre de disposer de câbles à paires torsadées à très haut débit.

Les supports de transmission (4/12)

- Caractéristiques des différentes catégories de câbles :
  - Les câbles de catégorie 1 et 2 fonctionnent sur une fréquence maximale inférieure à 10 MHz et permettent un débit maximal de 1 Mbit/s. Ils permettent le transport de la voix et des données.
  - Les câbles de catégorie 3 : fréquence maximale de 20 MHz, débit maximal de 16 Mbit/s. Utilisation : transport de la voix et des données, réseaux Ethernet.
  - Les câbles de catégorie 4 améliore le débit par rapport au Catégorie 3 (20 Mbit/s).
  - Les câbles de catégorie 5 (Norme EIA/TIA 568) : fréquence maximale de 100 MHz, débit maximal de 100 Mbit/s. Utilisation : transport de la voix et des données, réseaux Fast Ethernet.
  - Les câbles de catégorie 5 améliorée (5+ ou 5e) : fréquence maximale de 100 MHz, débit maximal de 155 Mbit/s. Utilisation : transport de la voix et des données, réseaux Fast Ethernet, réseaux ATM à 155 Mbit/s.

Les supports de transmission (5/12)

- Les nouvelles catégories de câbles :
  - Les câbles de catégorie 6 et 6a : fréquence maximale de 250 MHz, débit maximal de 2 Gbit/s. Utilisation : transport de la voix et des données, réseaux Fast Ethernet, réseaux Gigabit Ethernet, réseaux ATM à 155 Mbit/s, réseaux ATM à 622 Mbit/s.
  - Les câbles de catégorie 7 : fréquence maximale de 600 MHz, débit maximal de 10 Gbit/s. Utilisation : transport de la voix et des données, réseaux Gigabit Ethernet, réseaux ATM à 622 Mbit/s.
    Le câble catégorie 7 présente quatre paires torsadées individuellement et collectivement blindées afin de réduire les phénomènes parasitaires liés à la diaphonie.
    Ce type de câble s'associe avec les connecteurs GG45 compatible avec RJ45 et TERA (non compatible RJ45 et donc les catégories antérieures) utilisé de manière spécifique pour les applications où les exigences de sécurité sont importantes.

Les supports de transmission (6/12)

- Les câbles coaxiaux :
  - Un câble coaxial est un câble électrique constitué de deux conducteurs :
    - un conducteur cylindrique creux.
    - un fil électrique simple placé à l'intérieur du précédent et isolé par une matière non-conductrice.
  - La bande passante est inférieure à 100 MHz ce qui les rends inexploitables pour des réseaux hauts débits.
  - Le câble coaxial RG 58 :
    - connexion effectuée par des connecteurs BNC,
    - utilisé pour la transmission de données Ethernet dans la limite de 200 mètres,
    - voué à disparaître.

Les supports de transmission (7/12)

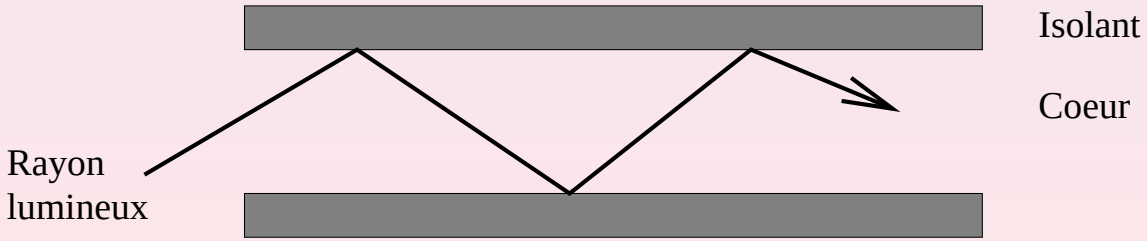
- Les câbles coaxiaux (suite) :
  - Le câble coaxial RG 11 :
    - câble coaxial épais : un meilleur niveau de blindage,
    - limitation à 500 mètres,
    - voué à disparaître au profit de la fibre optique.
  - Le cable coaxial large bande :
    - CATV : Community Antenna Television,
    - utilisé pour la transmission des chaînes de télévision par câble,
    - fréquence de largeur de bande pouvant aller jusqu'à 500 MHz, autorisant la transmission d'images.

Les supports de transmission (8/12)

- La fibre optique :
  - un cylindre constitué d'un matériau conduisant la lumière, enveloppé dans un isolant.
  - transmission par réfractions successives.
  - très large bande passante permettant des débits allant de 1 à plusieurs centaines de Gbit/s sur des distances de plusieurs kilomètres.
  - utilisation intéressante même dans des réseaux bas débit pour réduire le taux d'erreurs de transmissions et le nombre de retransmissions.
  - connexion à la fibre effectuée par un émetteur optique qui convertit un signal électrique en un signal lumineux.
  - 2 types de connecteurs possibles : SC (un ergot maintient le connecteur en place une fois enclenché) ou ST (le branchement est réalisé par un système à baïonnette).

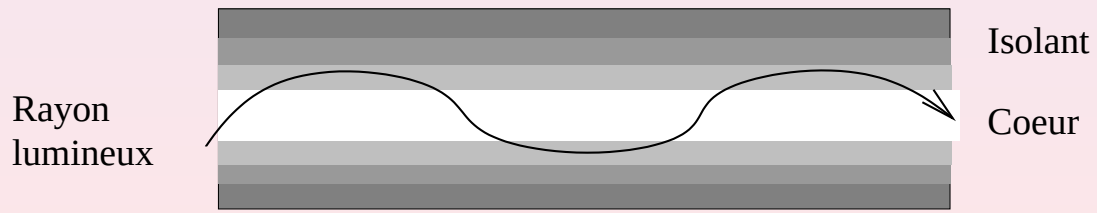
Les supports de transmission (9/12)

- La fibre optique (suite) :
  - Fibres multimodes à saut d'indice :
    - Le cœur translucide de la fibre est recouvert d'un matériau qui ne laisse pas passer la lumière (indice de réfraction nul).
    - Le rayon lumineux est transmis par réfractions successives.
    - Bande passante de 100 Mhz.
    - Adapté aux réseaux locaux hauts débits.
    - Le câble le moins cher pour les fibres optiques.



Les supports de transmission (10/12)

- La fibre optique (suite) :
  - Fibres multimodes à gradient d'indice :
    - L'indice de réfraction de la gaine n'est plus fixe (diminution en s'éloignant du cœur).
    - Chemin parcouru par le rayon plus court et donc diminution du temps de transmission.
    - Un coût de mise en œuvre plus important que les fibres à saut d'indice.



Les supports de transmission (11/12)

- La fibre optique (suite) :
  - Fibres monomodes :
    - Ne transmet que les rayons dont la trajectoire est l'axe de la fibre.
    - Un faisceau laser est nécessaire aux extrémités.
    - Les débits peuvent dépasser plusieurs dizaines de Gbit/s.
    - Un coût de mise en œuvre très élevé notamment à cause des faisceaux lasers.

Les supports de transmission (12/12)

- Les réseaux sans fils :
  - Utilisation de milieux comme l'air, le vide... comme support de transmission des ondes électromagnétiques : l'espace hertzien.
  - Plusieurs types d'ondes électromagnétiques sont utilisées dans les réseaux informatiques :
    - ondes radio : la gamme de fréquences va de 10 kHz jusqu'à 300 GHz. Pour les fréquences les plus basses, des architectures de réseaux locaux sans fils proposent des débits de 2 à 20 Mbit/s sur des distances atteignant 20 km. Pour les fréquences plus élevées, on peut atteindre des débits dépassant le Gbit/s.
    - ondes infrarouges : ondes de fréquences supérieures à 300 GHz. Leur création bien qu'assez simple est restreinte car à cette fréquence, elles ne peuvent traverser la matière physique.
    - ondes lumineuses : une source lumineuse (un laser) envoie des données à récepteur optique $\Rightarrow$ coût élevé.

Couche liaison de données (niveau 2)

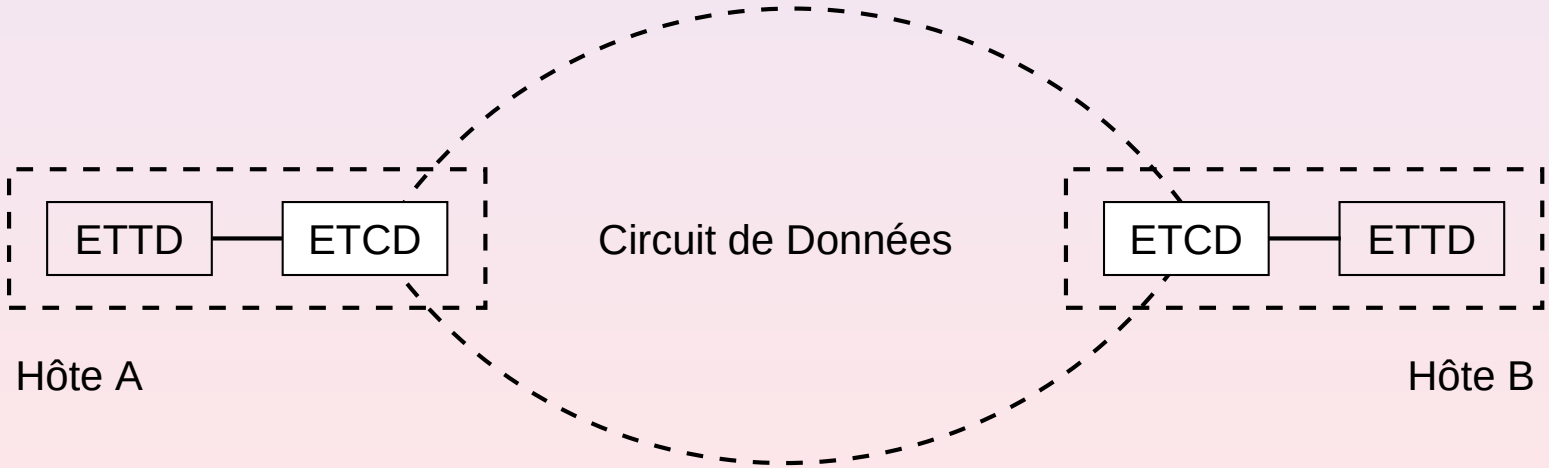
- Utiliser les services fournis par la couche physique.
- Les bits à envoyer sont regroupés en trames suivant un schéma précis :
  - taille de la chaîne binaire à envoyer,
  - champ de contrôle sur ces données,
  - formes des adresses des émetteurs et des récepteurs.
- La détection d'erreur permet de vérifier si une trame est arrivée sans avoir subie de modifications sur le média de transport.
- Certaines méthodes permettent de corriger les erreurs détectées.

Constitution des trames binaires

- Le récepteur doit être capable de reconstituer les trames à partir d'une chaîne binaire provenant du support physique.
- Pour cela il faut convenir d'un format de trames entre l'émetteur et le récepteur et plusieurs techniques peuvent être utilisées :
  - la taille en bits d'une trame est fixée,
  - la taille de la trame est transmise au destinataire,
  - des fanions sont utilisés pour repérer le début et la fin de la trame.

Commutation (1/2)

- Un réseau à commutation est un réseau longue distance qui propose des techniques permettant d'acheminer de manière optimisée des trames de niveau liaison de données.
- Utilisation d'ETTD et d'ETCD pour accéder au réseau.



Commutation (2/2)

- Commutateur :
  - un nœud réseau possédant plusieurs ports de connexion.
  - rôle : orienter les trames qu'il reçoit sur un port vers un autre port.
  - T_c (Temps de commutation) = Temps nécessaire pour mettre en place l'aiguillage au sein du commutateur.
- Méthodes de commutation :
  - Commutation de circuits.
  - Commutation de messages.
  - Commutation de paquets.
  - Commutation temporelle asynchrone.

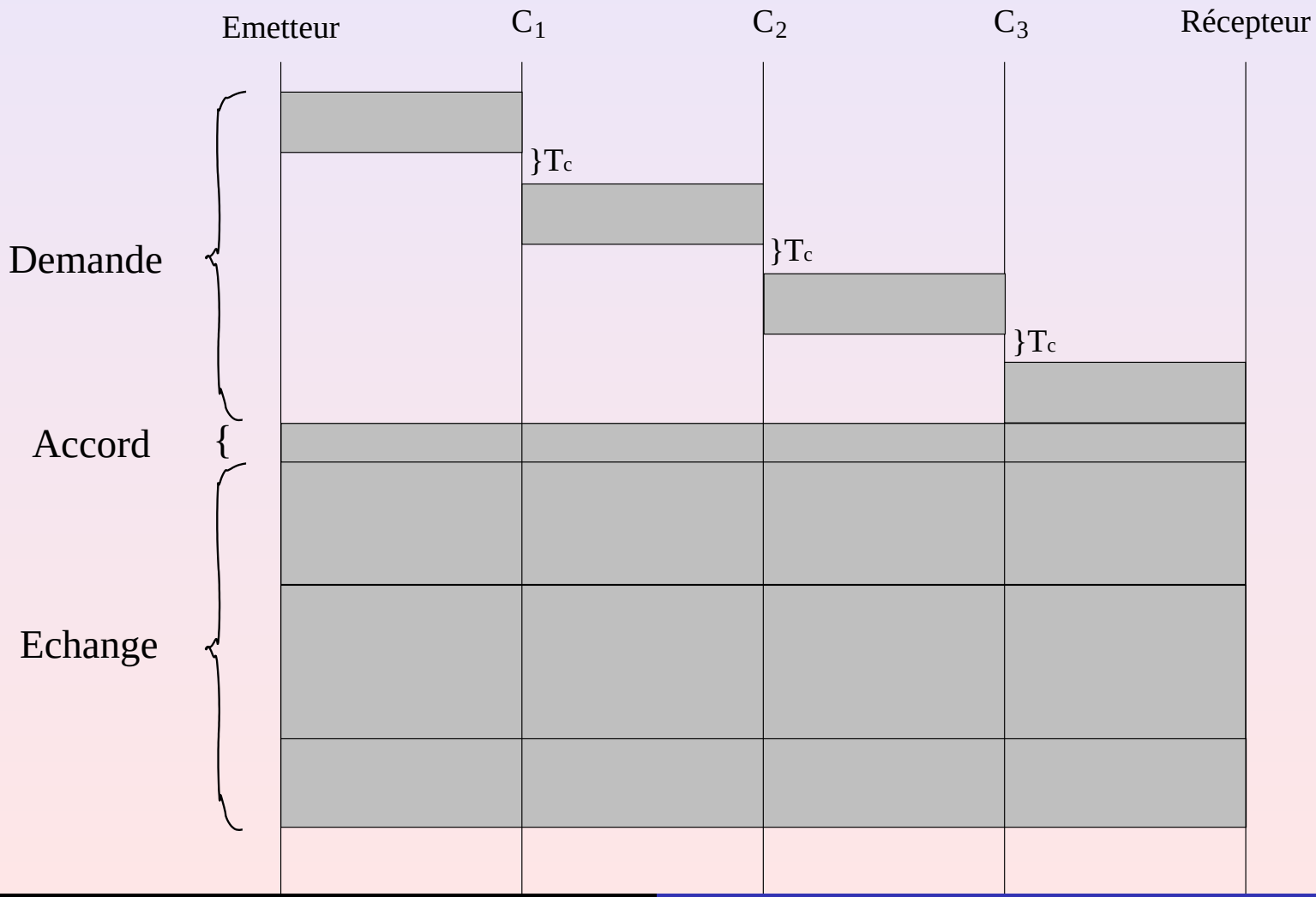
Commutation de circuits (1/3)

- L'envoi d'une trame nécessite la réservation d'un chemin physique à travers le réseau maillé.
- La communication s'effectue en trois phases :
  - établissement de la connexion (mise en place du circuit fixe entre les ETTD par les commutateurs).
  - le destinataire confirme la réception de la demande et accepte la connexion.
  - l'émetteur envoie les données par le circuit réservé.
- Avantages de la méthode :
  - Gain de temps lorsqu'il y a plusieurs envois : en effet l'aiguillage ne se fait qu'une seule fois dans les commutateurs (T_c).
  - Délai de transmission connus avant l'envoi des données = temps mis par la demande de connexion pour atteindre le destinataire.

Commutation de circuits (2/3)

- Inconvénients de la méthode :
  - Absence de dynamisme : un commutateur réservé pour un circuit n'est plus disponible tant que le dialogue n'est pas terminé.
  - Taux d'activité très faible : une seule ligne est utilisée entre deux commutateurs, les autres restent inoccupées.
- Utilisation de la méthode : le réseau téléphonique commuté (RTC).

Commutation de circuits (3/3)



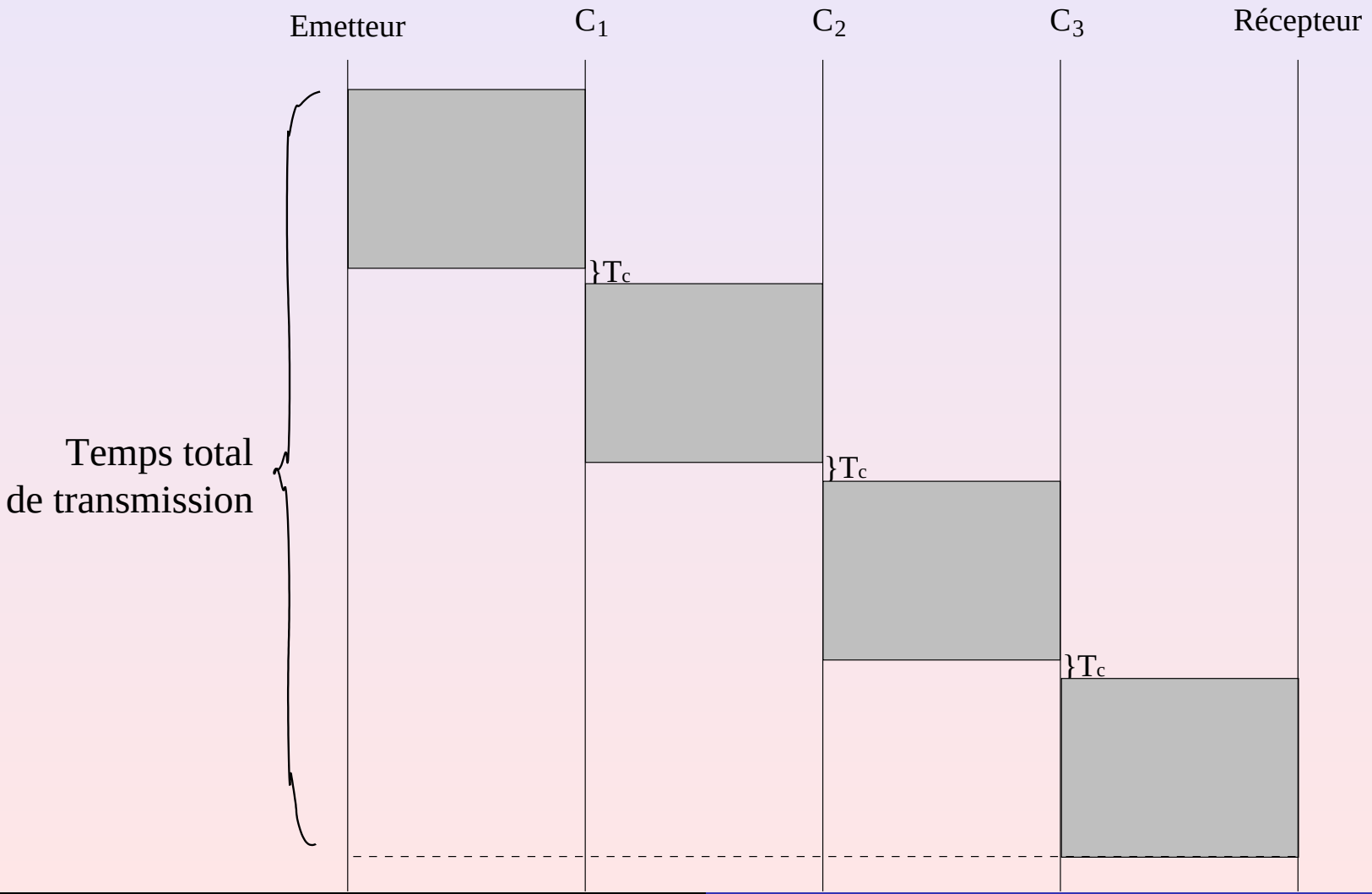
Commutation de messages (1/3)

- Pas d'établissement de connexion.
- Un message est transmis par la machine source au commutateur auquel elle est rattachée puis transmis de commutateur en commutateur jusqu'à la machine destinataire.
- Suppression de la phase de connexion :
  - $\Rightarrow$ gain de temps si peu d'échanges.
  - $\Rightarrow$ perte de temps si échanges plus nombreux car cumul des T_c.
- Le commutateur peut être utilisé pour d'autres communications car il ne reste pas bloqué durant toute la phase de dialogue.

Commutation de messages (2/3)

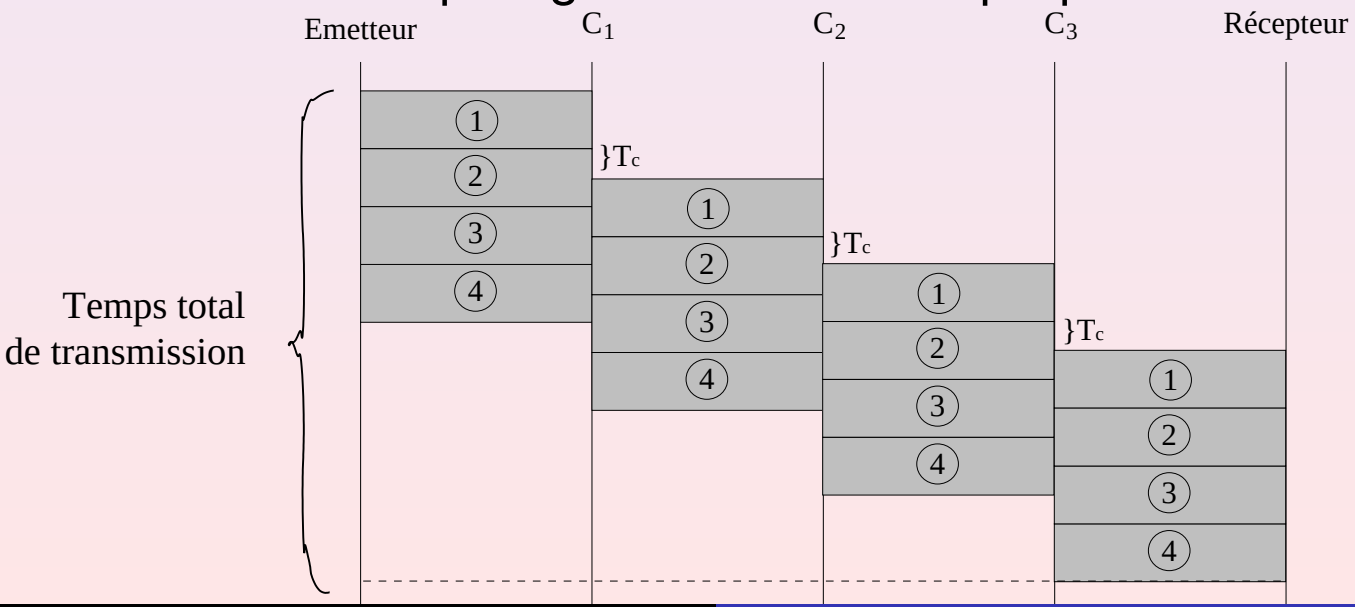
- En cas d'erreur, pas de trace du message émis dans les commutateurs, il faut donc demander à la source de réémettre le message
  - $\Rightarrow$ perte de temps
- Le temps de commutation (T_c) reste identique quelle que soit la taille du message $\Rightarrow$ envoi de longues chaînes binaires plus avantageux.

Commutation de messages (3/3)



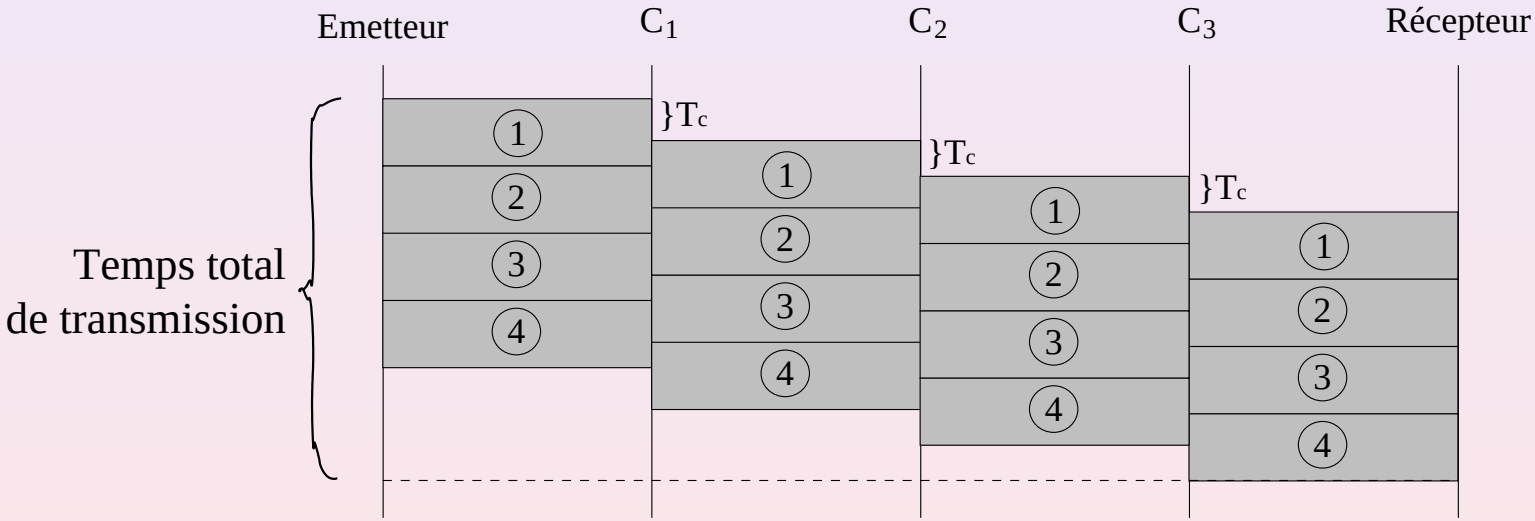
Commutation de paquets

- Similaire à la commutation de messages mais le message initial est découpé en entités plus petites appelées paquets.
- Chaque paquet est transmis à travers le réseau par commutateurs successifs.
- On obtient un gain de temps total pour l'acheminement car à un instant donné chaque ligne achemine un paquet différent.



Commutation temporelle asynchrone

- Comme pour la commutation de paquets, le message est découpé en plusieurs entités qui sont envoyées indépendamment les unes des autres.



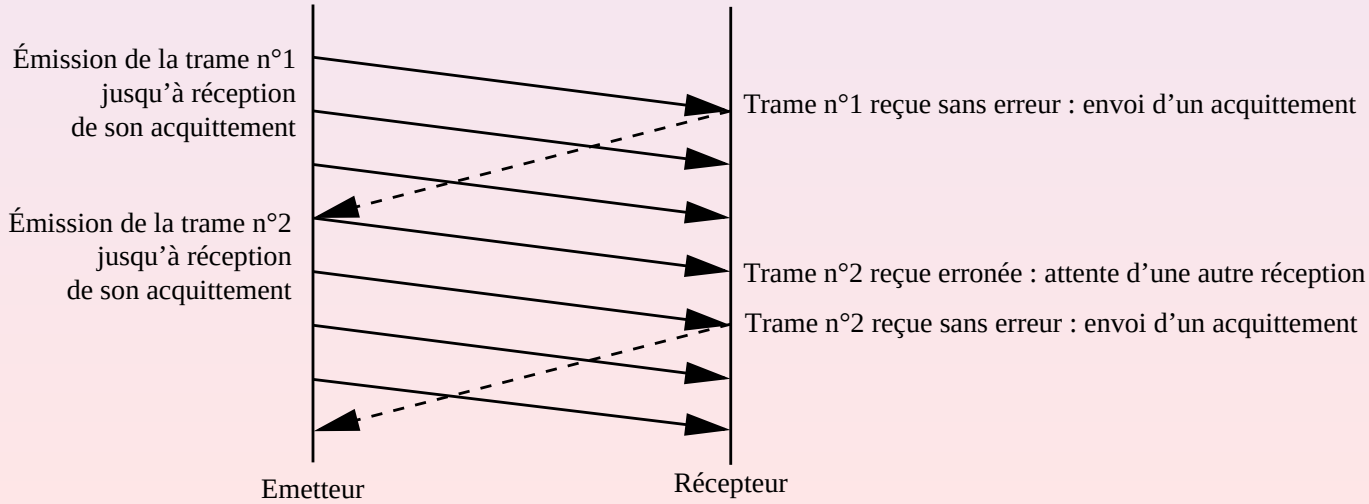
- Un commutateur peut commencer à émettre un paquet avant de l'avoir lu en entier.
- Cette technique est utilisée dans les réseaux ATM.

Gestion des erreurs de transmission

- Objectif : rendre transparent les erreurs de transmission de trames aux couches supérieures.
- La détection des erreurs doit être faite au niveau des ETTD et des ETCD.
- Détection des erreurs :
  - Signaler qu'une trame reçue est différente de celle envoyée.
  - Bit de parité.
  - Code CRC (Code de Redondance Cyclique).
- Correction des erreurs :
  - Transmettre des données supplémentaires qui permettront éventuellement de corriger les trames erronées.
  - Code de Hamming.
  - Code de Reed-Salomon.

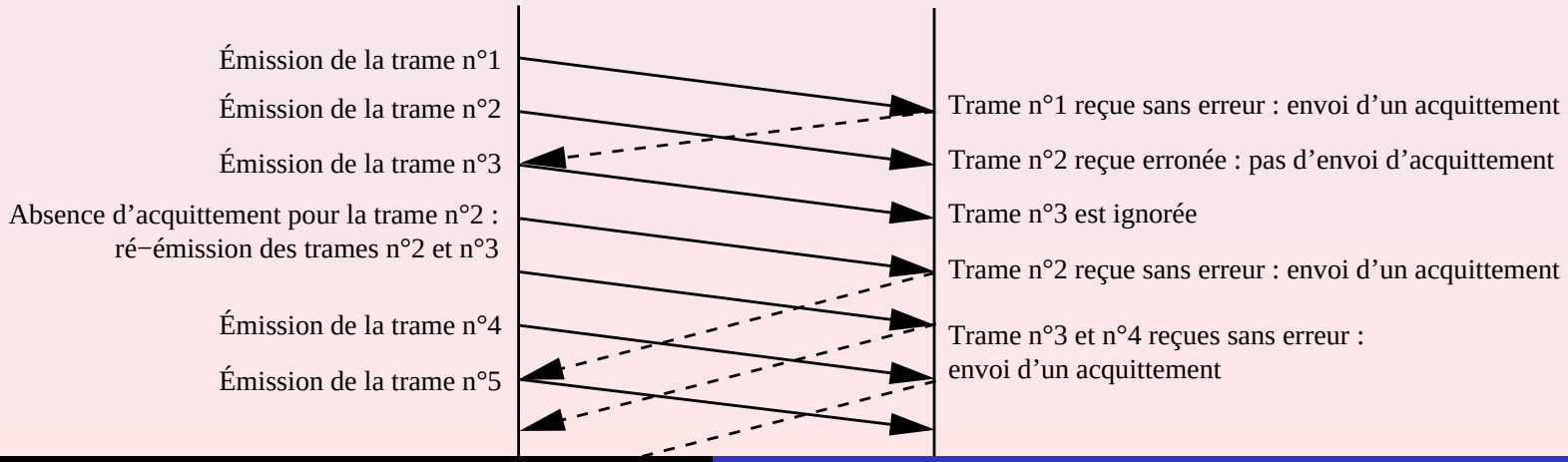
Gestion des acquittements (1/3)

- Problèmes des erreurs :
  - Deux types d'erreurs peuvent se produire : détection d'une erreur de transmission (cf. précédemment) et perte d'une trame.
  - Comment être sûr que les trames sont arrivées (ou pas) correctement au destinataire $\Rightarrow$ par l'envoi d'un message d'acquittement à l'émetteur.
- Protocole d'attente/réponse (Send and Wait) :
  - envoi d'une trame jusqu'à la réception d'un acquittement



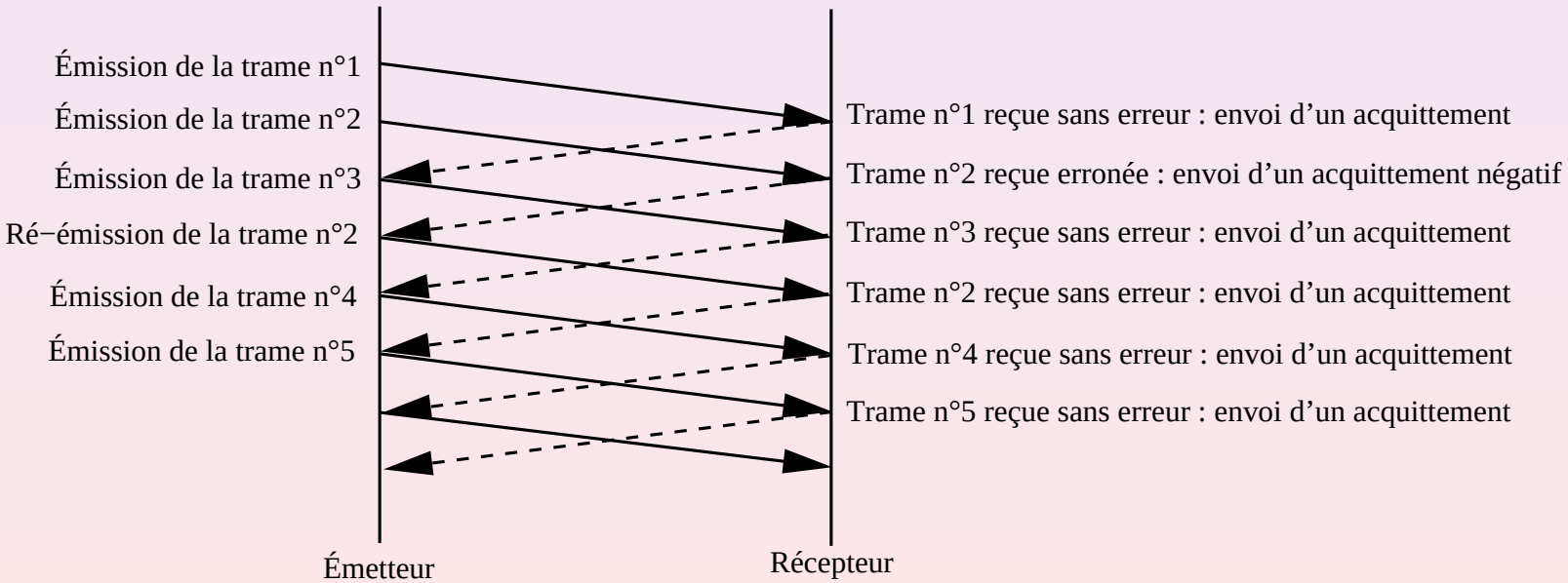
Gestion des acquittements (2/3)

- Transmission avec anticipation, retransmission en continu
  - trames envoyées les unes après les autres
  - une trame arrive sans erreur ⇒ envoi d'un acquittement pour la trame
  - une trame arrive erronée ⇒ pas d'envoi d'acquittement et les trames suivantes ignorées jusqu'à la réémission de la trame erronée
  - même ordre de traitement des trames coté émetteur et coté récepteur



Gestion des acquittements (3/3)

- Transmission avec anticipation, retransmission sélective
  - similaire au protocole précédent
  - une trame arrive erronée $\Rightarrow$ envoi d'un acquittement négatif
  - on ne réémet que les trames erronées



Le protocole HDLC

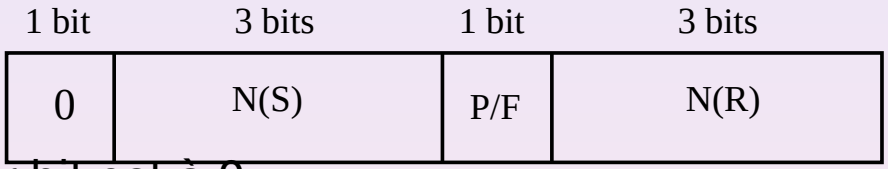
- High-level Data Link Control
- Protocole de base qui a servi à mettre en place LAP-D, LAP-D, LAP-F et PPP
- Format des trames binaires utilisées par HDLC :

8 bits	8 bits	8 bits	*n* bits	16 bits	8 bits
Fanion de début	Adresse destination	Commandes	Données	Contrôle d'erreur	Fanion de fin

  - Le *Fanion de début* et le *Fanion de fin* indique les deux extrémités de la trame : ils sont constituées de la chaîne 01111110.
  - L'*Adresse de destination* identifie l'ETTD destinataire.
  - *Commande* = informations nécessaires à l'interprétation de la trame.
  - Suivant le rôle de la trame, *Données* = une chaîne binaire ou non.
  - Le *Contrôle d'erreur* est réalisé par un code CRC basé sur le polynôme générateur $G(x) = x^{16} + x^{12} + x^5 + 1$.

Différents types de trames (1/3)

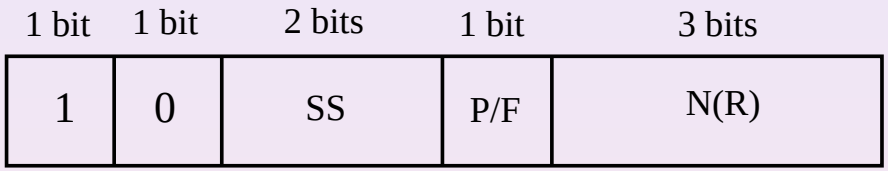
- *Commandes* ⇒ spécification du type des trames.
- Trame d'information



  - Le premier bit est à 0.
  - Le champ *Données* n'est pas vide.
  - N(S) est le numéro de la trame émise.
  - Le bit P/F peut être interprété de 4 façons différentes selon que
    - la trame provient de l'initiateur de l'échange (P) :
      ⇒ P=0 : l'initiateur n'attend pas de réponse à cette trame.
      ⇒ P=1 : l'initiateur attend une réponse à cette trame.
    - la trame provient du correspondant (F) :
      ⇒ F=0 : le correspondant n'a pas terminé d'émettre des trames.
      ⇒ F=1 : le correspondant a terminé ses envois de trames.
  - N(R) : acquittement de toutes les trames dont le numéro < N(R).

Différents types de trames (2/3)

- Trame de supervision

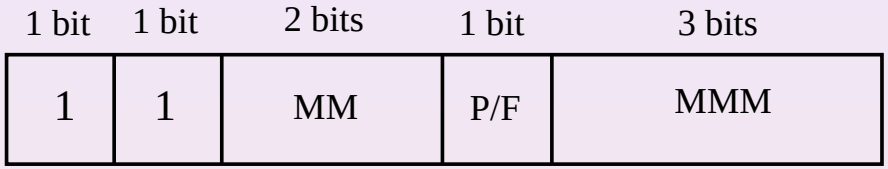


  - Le premier bit est à 1 et le second bit est à 0.
  - Le champ *Données* n'est pas vide.
  - Les deux bits *SS* informent le destinataire de certaines requêtes de l'émetteur :

00	RR *ReceiveReady*	Acquittement de toutes les trames de numéro inférieur à N(R) : en attente de réception de trames
01	REJ *Reject*	Demande de rejet de toutes les trames de numéro supérieur à N(R)
10	RNR *ReceiveNotReady*	Demande d'une suspension des envois de trames après la trame de numéro N(R)
11	SREJ *SelectiveReject*	Rejet de la trame N(R) et demande de retransmission de celle-ci

Différents types de trames (3/3)

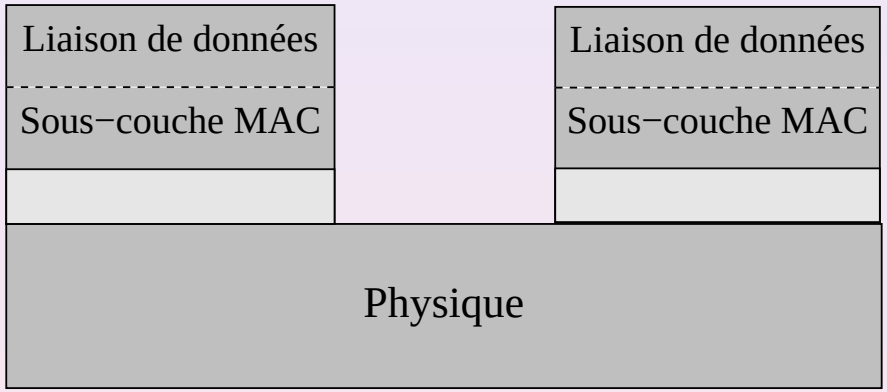
- Trame de supervision non numérotée



  - Elles ont pour rôle de gérer la mise en place et le relâchement de la connexion.
  - Elles permettent d'envoyer des données en mode datagramme.
  - Les différents types de trames non numérotées (valeurs de MM et MMM) sont : SABME (11,110), DISC (00,010), UA (00,110), DM (11,000), FRMR (10, 001), XID (11, 101), TEST (00,111), UI (00,000), AC0 Commande (10,110), AC1 Commande (10,111), AC0 Réponse (10,110), AC1 Réponse (10,111).

La sous-couche MAC (niveau 2)

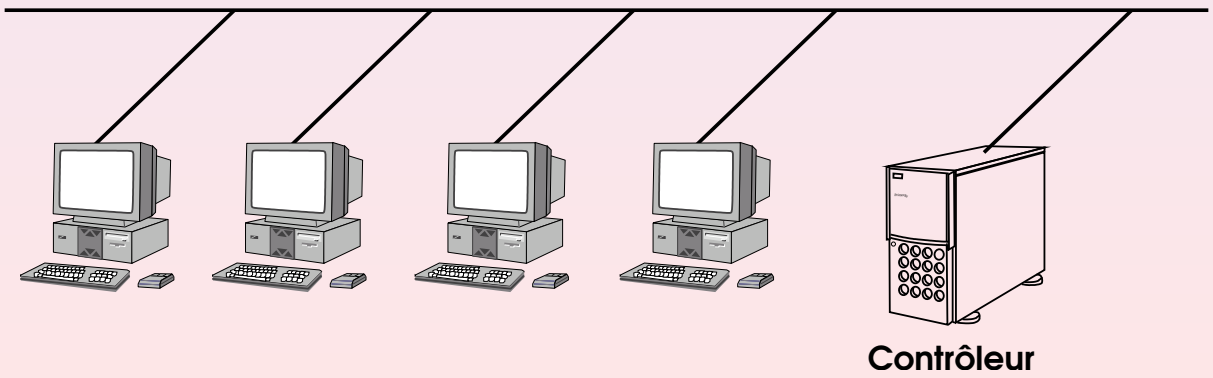
- MAC : Medium Access Control



- Elle regroupe toutes les fonctions de niveau liaison de données chargées du contrôle d'accès au support.
- Nous allons voir :
  - les méthodes d'accès au support,
  - les normes de réseaux,
  - et les ponts.

Les méthodes d'accès au support (1/9)

- Méthodes sans collision (1/3) :
  - L'allocation centralisée :
    - Un élément actif (contrôleur) interroge une à une toutes les machines connectées et en fonctionnement.
    - Si une machine veut émettre une trame, elle soumet sa requête puis le contrôleur lui octroie le support.
    - Lorsque l'émission est terminée, la machine le signale au contrôleur qui peut alors procéder à une nouvelle allocation du support physique.

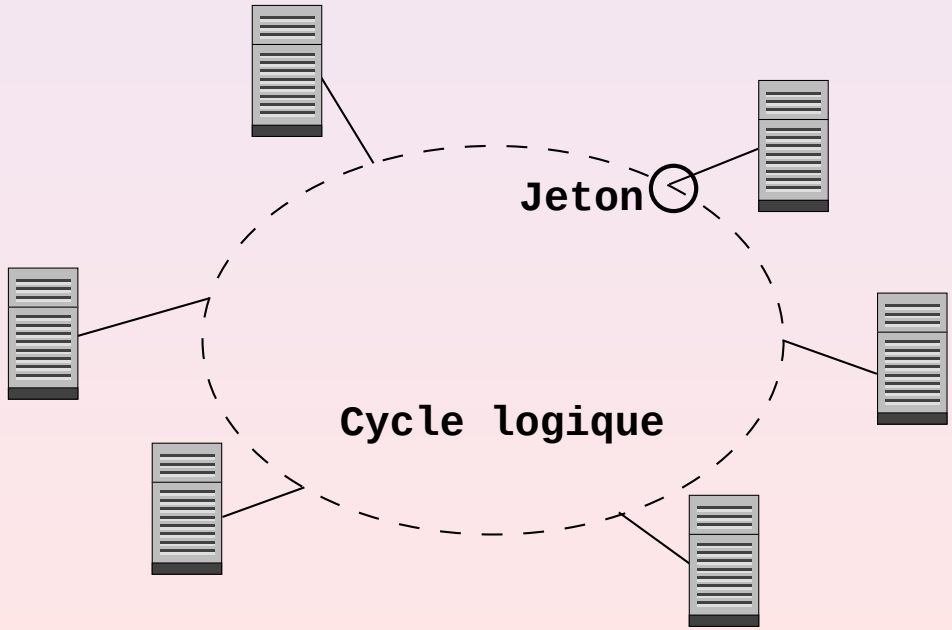


Les méthodes d'accès au support (2/9)

- Méthodes sans collision (2/3) :
  - La méthode Bip-Map :
    - Utilisation systématique d'une période de contention = un intervalle de temps pendant lequel aucune communication ne peut avoir lieu.
    - La période de contention est découpée en autant d'intervalles qu'il y a d'ordinateurs connectés.
    - Lorsqu'une machine veut émettre, elle le signale pendant la période de contention qui lui est allouée.
    - Lorsque la période de contention est terminée, chaque ordinateur qui en a fait la demande peut alors émettre pendant une période de transmission qui lui est réservée.

Les méthodes d'accès au support (3/9)

- Méthodes sans collision (3/3) :
  - L'allocation distribuée :
    - L'autorisation d'émettre est directement donnée par un jeton qui circule sur le réseau de façon cyclique.
    - Lorsqu'une machine veut émettre, elle conserve le jeton lors de son passage sinon elle le réémet sur le support.



Les méthodes d'accès au support (4/9)

- Méthodes avec collision (1/6) :
  - La méthode ALOHA :
    - Émission sur le support des données sans aucune action préalable.
    - L'émetteur écoute ensuite le support pour savoir s'il y a eu collision.
    - S'il y a eu collision, l'émetteur attend un moment puis renvoie la trame.
    - Il existe plusieurs variantes de la méthode ALOHA :
      L'émission peut ne pas se faire de façon entièrement libre mais à des instants précis.
      L'élément actif doit pour cela posséder une horloge pour pouvoir découper le temps en intervalles réguliers.
      Lorsqu'un ordinateur veut émettre une trame, il attend le signal d'horloge suivant.

Les méthodes d'accès au support (5/9)

- Méthodes avec collision (2/6) :
  - La méthode CSMA 1-persistant :
    - Basée sur l'écoute préalable du média de transmission avant l'émission d'une trame.
    - CSMA=Carrier Sense Multiple Access (Accès Multiple à Détection de Porteuse).
    - Avant de transmettre une trame, l'ordinateur émetteur, en réalité son interface réseau, écoute si le support véhicule un signal :
      si c'est le cas, il n'émet pas car cela provoquerait une collision mais il continue d'écouter le support. Lorsque le support est libre, il envoi la trame.
      si le support est libre la trame est immédiatement transmise et l'écoute est coupée.

    $\Rightarrow$ solution simple mais peu performante, le support reste occupé pendant toute la phase d'émission d'un ordinateur.

Les méthodes d'accès au support (6/9)

- Méthodes avec collision (3/6) :
  - La méthode CSMA non persistant :
    - Lorsque l'émetteur constate que le média est occupé, il ne reste pas à l'écoute mais réessayera plus tard.
  - La méthode CSMA/CD :
    - Elle est basée sur le CSMA non persistant.
    - Lorsque l'émetteur écoute le support, il peut ne pas détecter la présence d'un signal à cause d'une distance trop grande.
    - Une collision ne va pas se produire immédiatement mais plus tard.
    - Une seconde phase au CSMA non persistant a donc été ajoutée afin de résoudre ce problème.
    - Après l'émission de la trame, l'émetteur reste à l'écoute du support afin de détecter une éventuelle collision.

    $\Rightarrow$ CSMA/Collision Detection
    - Lors d'une collision la trame est alors réémise après un temps d'attente aléatoire.

Les méthodes d'accès au support (7/9)

- Méthodes avec collision (4/6) :
  - La méthode CSMA/CD (suite) :
    - Lors d'une collision la trame est alors réémise après un temps d'attente aléatoire.
    - Mise en place dans les réseaux locaux Ethernet, Fast Ethernet et Gigabit Ethernet.

    $\Rightarrow$ méthode de référence.
    - Une évolution a été proposée : CSMA/CRCD. Elle permet d'obtenir de meilleures performances mais elle est plus complexe à mettre en œuvre. CR=Contention Resolution.
  - La méthode CSMA/CA :
    - CSMA Collision Avoidance.
    - Méthode mise en place pour les environnements sans fil où la méthode CSMA/CD ne peut pas marcher.

Les méthodes d'accès au support (8/9)

- Méthodes avec collision (5/6) :
  - La méthode CSMA/CA (suite) :
    - Mécanisme d'esquive de collision basé sur un principe d'accusé/réception réciproque entre l'émetteur et le récepteur.
    - Écoute du réseau puis émission de la trame différée si le réseau est encombré.
    - Si le support de transmission est libre pendant un temps donné (appelé DIFS pour Distributed Inter Frame Space), alors on peut émettre.
    - La station transmet un message appelé Ready To Send (noté RTS signifiant prêt à émettre) contenant des informations sur le volume des données qu'elle souhaite émettre et sa vitesse de transmission.
    - Le récepteur (généralement un point d'accès) répond un Clear To Send (CTS, signifiant le champ est libre pour émettre), puis la station commence l'émission des données.

Les méthodes d'accès au support (9/9)

- Méthodes avec collision (6/6) :
  - La méthode CSMA/CA (suite et fin) :
    - À réception de toutes les données émises par la station, le récepteur envoie un accusé de réception (ACK).
    - Toutes les stations avoisinantes patientent alors pendant un temps qu'elles considèrent être celui nécessaire à la transmission du volume d'information à émettre à la vitesse annoncée.
  - La méthode RTS/CTS :
    - Request To Send/Clear To Send.
    - Sonder et réserver le support par un cours échange avec le récepteur.
    - Si l'échange aboutit, les autres ordinateurs ayant observé le signal attendent leur tour pour réserver le support.
    - Méthodes conçues pour les réseaux locaux sans fils.

Les normes de réseaux (1/12)

- La norme 802.3 et l'architecture Ethernet :
  - Elle définit les réseaux locaux utilisant la méthode CSMA/CD.
  - Le support choisi est un bus logique auxquels sont connectés tous les éléments actifs.
  - Les réseaux locaux 802.3 proposent un débit binaire théorique de 10 Mbit/s.
  - Les trames émises suivent un format précis permettant une gestion optimisée et un contrôle d'erreur fiable. Elles sont émises toutes les 96 μs.

7 octets	1 octet	6 octets	6 octets	2 octets	0 − 1500 octets	0 − 46 octets	4 octets
Préambule	Délimiteur de trame	Adresse destination	Adresse source	Longueur champ données	Données	PAD	Contrôle d'erreur

  - Ethernet est une norme de LAN qui respecte les spécifications de la norme 802.3.

Les normes de réseaux (2/12)

- La trame 802.3 est composée de huit champs :
  - *Préambule* : il sert à synchroniser l'émetteur et le récepteur en envoyant une suite de bits 10.
  - Le *Délimiteur de trame* sert à identifier le début des données utiles.
  - Les champs *Adresse destination* et *Adresse source* (adresses MAC) sont utiles pour déterminer le récepteur en mode diffusion et l'acheminement de la trame.
  - Les champs *Données* étant de longueurs variables, le champ *Longueur du champ de données* permet au récepteur d'interpréter correctement les champs *Données*, *PAD* et *Contrôle d'erreur*.
  - La longueur d'une trame est comprise entre 64 et 1518 octets. Si la quantité de données est trop faible le champ PAD est ajouté.
  - Le *Contrôle d'erreur* est réalisé par un CRC-32. En cas d'erreur le récepteur redemande la transmission de la trame dans la limite de 16 essais.

Les normes de réseaux (3/12)

- La norme 802.3u et l'architecture Fast Ethernet :
  - Évolution de la norme 802.3 pour permettre un débit de 100 Mbit/s.
  - Elle est aussi appelé norme 802.14.
  - Elle s'appuie sur trois types de câblage : le câble à paires torsadées de Catégorie 3 ou de Catégorie 5 et la fibre optique.
  - Trois classes de réseau Fast Ethernet ont été créées relativement au type de câblage :
    - La classe 100BaseT4 qui s'appuie sur des câbles à paires torsadées de Catégorie 3. Cela permettait de pouvoir réutiliser le câblage lors de passage d'un réseau Ethernet vers un réseau Fast Ethernet. La longueur maximale d'un segment est de 100 m.
    - La classe 100BaseTX qui s'appuie sur des câbles à paires torsadées de Catégorie 5. La longueur maximale d'un segment est de 100 m.
    - La classe 100BaseFX qui s'appuie sur 2 fibres optiques. La longueur maximale d'un segment est de 2000 m.

Les normes de réseaux (4/12)

- La norme 802.3z et l'architecture Gigabit Ethernet :
  - Elle s'appuie toujours sur la norme 802.3 et permet des débits de 1000 Mbit/s.
  - Trois classes de transmission ont été définies :
    - La classe 1000BaseTX : elle s'appuie sur des câbles à paires torsadées de catégorie 5, 6 ou 7. La longueur maximale d'un segment est de 100 m.
    - La classe 1000BaseSX : elle s'appuie sur des fibres optiques multimodes à 62.5 μm (longueur maximale d'un segment : 275 m) ou 50 μm (longueur maximale d'un segment : 550 m).
    - La classe 1000BaseLX : elle peut s'appuyer sur des fibres optiques multimodes à 62.5 μm ou 50 μm (longueur maximale d'un segment : 550 m dans les deux cas) mais elle peut aussi utiliser des fibres optiques monomodes à 10 μm. Dans ce dernier cas la longueur maximale d'un segment est alors de 10 km.

Les normes de réseaux (5/12)

- La norme 802.4 et l'architecture Token Bus :
  - Utilisation de la méthode d'allocation distribuée.
  - Réseaux de type bus à jeton.
  - Utilisation de câbles coaxiaux (75 Ω ou CATV) pour des débits allant de 1 à 10 Mbits.
  - La gestion du bus est confiée à un élément actif appelé superviseur qui crée le jeton lors de l'initialisation du réseau et se charge de sa circulation entre les ordinateurs.
  - Le superviseur détermine un ordre cyclique de passage du jeton entre tous les postes connectés ce qui revient à l'utilisation d'un anneau logique.

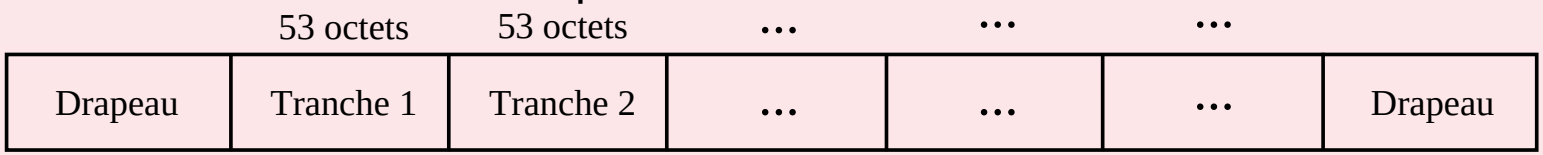
n octets	1 octet	1 octets	2 ou 6 octets	2 ou 6 octets	< 8192 octets	4 octets	1 octets
Préambule	Délimiteur	Type de trame	Adresse destination	Adresse source	Données	Contrôle d'erreur	Délimiteur

Les normes de réseaux (6/12)

- La norme 802.5 et l'architecture Token Ring :
  - Simplification de la norme 802.4 et suppression de l'utilisation d'un superviseur.
  - Réseau de type anneau à jeton.
  - Remplacement du support physique en bus par un anneau.
  - Trois types de câbles peuvent être employés :
    - Câbles à paires torsadées non blindés : 1 Mbit/s à 4 Mbit/s et utilisation du Manchester différentiel.
    - Câbles à paires torsadées blindés : 1 Mbit/s à 16 Mbit/s et utilisation du Manchester différentiel.
    - Fibres optiques : 1 Mbit/s à 16 Mbit/s et utilisation du Manchester différentiel.

Les normes de réseaux (7/12)

- La norme 802.6 :
  - Aussi appelée DQDB (Distributed Queue Dual Bus), elle a été créée spécifiquement pour les MAN.
  - Basée sur un double bus physique, elle permet l'interconnexion d'un nombre important de postes de travail sur des distances allant jusqu'à plusieurs kilomètres.
  - Les supports utilisés sont le câble coaxial ou la fibre optique en fonction de la distance à parcourir.
  - Un générateur de trames est connecté à chaque bus et il a pour rôle d'émettre des trames vides à intervalles de temps réguliers (125 μs).
  - Les trames sont divisées en tranches de 53 octets pour un nombre de tranches pouvant aller de 54 à 59.



Les normes de réseaux (8/12)

- La norme 802.6 (suite) :
  - Le format d'une tranche est le suivant :

1 octet	4 octets	48 octets
Trame de contrôle d'accès	Marque de début	Données

  - Les ordinateurs souhaitant émettre réservent des tranches libres pour émettre leurs données.
  - Cette architecture de réseau est compatible avec la commutation ATM (même temps de transmission inter-trames : 125 μs).

Les normes de réseaux (9/12)

- La norme 802.11 et les architectures sans fils
  - Architecture de réseaux locaux sans fils basée sur une technologie radio.
  - L'interface réseau prend la forme d'une station de base à laquelle est connectée une antenne.
  - Le débit binaire, fixé par cette norme, est limité à 3 Mbit/s mais de nouvelles versions de cette norme permettent des débits plus conséquent :
    - 802.11b : débit de 11 Mbit/s (802.11b+ $\rightarrow$ 22 Mbit/s).
    - 802.11a et 802.11g : débit de 54 Mbit/s.
    - 802.11g+ : débit de 108 Mbit/s.
    - 802.11n : débit de 302 Mbit/s.
  - La méthode d'accès au support est CSMA/CA et optionnellement RTS/CTS.

Les normes de réseaux (10/12)

- La norme FDDI
  - Fiber Distributed Data Interface.
  - Destinée aux réseaux LAN et MAN haut débit.
  - Elle est basée sur un double anneau en fibres optiques dont la circonférence maximale est de 200 km.
  - Un sens de transmission pour chacun de ces deux anneaux.
  - Les machines dont le nombre peut atteindre 1000 sont connectées aux deux anneaux.
  - En cas de panne, le réseau peut fonctionner avec un seul anneau et une procédure de dépannage est lancée.
  - L'accès à un anneau se fait par la méthode du jeton.

Les normes de réseaux (11/12)

- La norme Frame Relay :
  - Réseau à commutation de paquets autorisant des débits très élevés et des transferts fiables (très bonne gestion des erreurs).
  - Permet le multiplexage sur une même ligne de transmission.
  - Permet le transfert des données, des images ou de la voie.
  - Utilisée pour l'interconnexion de réseaux distants.
  - Il offre la possibilité de véhiculer des paquets issus de protocoles différents tels que TCP/IP ou IPX.
  - Le débit binaire peut aller de 56 Kbits/s jusqu'à 2 Mbit/s.
  - La gestion de l'accès au support est fait par le protocole RSVP (Protocole de Réservation de Ressources).

Les normes de réseaux (12/12)

- Le système GSM :
  - Global System for Mobil communications : système européen de communication sans fil, basé sur une technologie de transmission par paquets radio.
  - La première version du GSM utilisait la bande des 900 MHz (GSM 900) mais une saturation de cette bande a entraîné la réservation de la bande des 1800 MHz.
  - Les différents éléments constituant le réseau sont les stations mobiles (téléphones portables), les stations de base et le centre de gestion chargé de faire le lien avec le réseau fixe.

Les ponts

- Un pont est un élément d'électronique permettant d'interconnecter des réseaux locaux dont la couche physique et la sous-couche MAC diffèrent (répondant à des normes réseaux différentes).
- Conversion des trames arrivant d'un réseau dans un format compréhensible par un autre réseau.
- Un pare-flamme (firewall) est un pont particulier permettant de mettre en place de la sécurité entre deux réseaux dont les normes peuvent être identiques ou non.

Couche réseau (niveau 3)

- Elle a en charge d'acheminer les paquets à travers le maillage du réseau.
- Ses principales fonctions concernent l'adressage des éléments constitutifs du réseau et le routage de l'information.
- Elle est présente dans le modèle TCP/IP. Ses fonctions principales sont regroupées au sein du protocole IP.

Le routage (1/5)

- Datagramme ou circuit virtuel :
  - Mode sans connexion :
    - Les données envoyées sont découpées en paquets (taille fixe ou non selon les protocoles) appelés datagrammes.
    - Les datagrammes sont acheminés indépendamment les uns des autres.
    - Aucun contrôle sur le flux d'information n'est effectué (pas d'évaluation préalable du trafic ou de la qualité du transfert).
  - Mode orienté connexion :
    - Phase d'établissement de la connexion préalable à l'envoi des données : un circuit virtuel est mis en place.
    - Toutes les données émises emprunteront le même chemin.
    - L'acquittement depuis le récepteur se fait par le même circuit virtuel.

Le routage (2/5)

- Principe du routage :
  - Son rôle : acheminer un paquet de données à travers le réseau.
  - Fonction présente dans chaque nœud du maillage.
  - Pour chaque paquet qui arrive sur l'un de ses ports en entrée, la fonction de routage choisie de façon déterministe le port de sortie vers lequel envoyer le paquet.
  - Deux classes d'algorithmes de routage :
    - les algorithmes non adaptatifs utilisent des routes statiques et ne tiennent pas compte de l'état des lignes de transmission.
    - les algorithmes adaptatifs précédent tout envoi de données par une étude préalable du contexte. On parle de routage dynamique. Ils sont plus complexes à mettre en œuvre mais permettent de meilleures performances.

Le routage (3/5)

- Algorithmes (1/3) :
  - Routage par inondation :
    - la technique la plus utilisée en mode diffusion.
    - un datagramme reçu par un routeur sur un de ses ports est réémis sur tous les autres ports.

    $\rightarrow$ cela engendre un trafic très important.
  - Routage du plus court chemin :
    - Représentation du maillage du réseau sous forme d'un graphe.
    - Les routeurs représentent les sommets et les lignes de transmission les arêtes.
    - On associe des coûts aux lignes de transmission, on obtient alors un graphe valué.
    - La recherche du plus court chemin consiste donc à trouver la chaîne d'arêtes dont la somme est minimale.
    - Le coût d'un chemin peut être fonction du nombre de routeurs traversés, de la distance géographique, d'une évaluation du trafic réseau, etc.

Le routage (4/5)

- Algorithmes (2/3) :
  - Routage à vecteur de distance :
    - L'un des premiers algorithmes de routage dynamique.
    - Chaque élément actif possède en mémoire une table de routage propre qui lui indique pour chaque destination connue le port de sortie à utiliser et un port par défaut pour les destinations inconnues.
    - Des communications inter-routeurs permettent de mettre à jour la table de routage locale à partir de celle de ses voisins.
    - La taille des tables de routage des stations émettrices ou réceptrices est limitée mais la table de routage des routeurs peut comporter de nombreuses entrées.

Le routage (5/5)

- Algorithmes (3/3) :
  - Routage hiérarchique :
    - Basé sur la technique de routage à vecteur de distance.
    - Objectif : limiter le nombre d'entrées à consulter lors de la recherche séquentielle d'un destinataire.
    - Solution : diviser le réseau en zones géographiques appelées régions.
    - Trois types de données dans la table de routage :
      le port à utiliser en sortie pour les destinataires situés dans la même région,
      les ports de sortie servant à accéder à chacune des autres régions du réseau,
      un port pour les destinataires inconnus.

Le protocole IP

- Un protocole de communication universel permettant l'interconnexion de systèmes hétérogènes, indépendamment des supports de transmission, de la nature de l'architecture réseau, des systèmes d'exploitation ou des applications utilisées.
- Le protocole de communication le plus répandu à l'heure actuelle.
- Il fait partie intégrante de l'architecture TCP/IP.
- Souvent associé au protocole de transport TCP, il peut néanmoins communiquer avec d'autres protocoles de niveau transport.
- Sa version actuelle est IPv4 mais une nouvelle version (IPv6) normalisée depuis 1995 devrait très bientôt la remplacer.

Le datagramme IP (1/4)

- IP propose un service non fiable et sans connexion.
- IP véhicule des entités (datagramme IP) entre deux éléments du réseau.
- En cas de constat d'erreur dans le datagramme, il n'est pas remis à la couche supérieure (transport) et une demande de réémission est effectuée.
- Chaque datagramme est routé de façon indépendante, et l'ordre de réception peut différer de l'ordre d'émission à cause de problèmes de trafic sur une ligne de transmission, d'erreurs de transmission, etc.

Le datagramme IP (2/4)

- Format du datagramme IP (1/3) :

4 bits	4 bits	8 bits	16 bits	16 bits
Version	Longueur de l'entête	Type de service	Longueur totale	Identificateur
4 bits	12 bits	4 bits	8 bits	16 bits
Drapeau	Position du fragment	Durée de vie	Protocole	Total de contrôle de l'entête
32 bits	32 bits	< 32 bits	0 − 32 bits	n bits
Adresse source	Adresse destination	Options	Bourrage	Données

- La taille des datagrammes IP ne doit pas excéder 65536 octets.
- Il faut donc scinder les paquets en provenance de la couche transport dont la taille est trop grande en fragments IP.

Le datagramme IP (3/4)

- Format du datagramme IP (2/3) :
  - *Version* : il indique par quel protocole IP le datagramme a été créé ce qui permet de faire cohabiter par exemple le protocole IPv4 et IPv6 sur un même réseau.
  - *Longueur de l'en-tête* : il permet de détecter la présence ou non du champ option.
  - *Type de service* : il définit la qualité de service demandée pour le datagramme : rapidité, absence d'erreur, priorité...
  - *Longueur totale* : la taille d'un datagramme n'étant pas fixe mais limitée à 65536 octets, ce champ consigne la taille du datagramme émis.
  - *Drapeau, Identification, Position du fragment* : le *Drapeau* permet de savoir si le datagramme est fragmenté ou non. S'il est fragmenté le champ *Identification* indique à quel datagramme appartient le fragment et sa position sera connue au moyen du champ *Position du fragment*.

Le datagramme IP (4/4)

- Format du datagramme IP (3/3) :
  - *Durée de vie* : elle permet de limiter dans le temps la présence d'un datagramme sur le réseau Internet, elle décrémente chaque fois que le datagramme traverse un routeur.
  - *Protocole* : il spécifie le protocole de niveau transport à l'origine de l'émission afin d'être traité par le même protocole à la réception.
  - *Total de contrôle de l'en-tête* : il permet de détecter des erreurs de transmission survenues sur les champs de l'en-tête. La validité des données n'est pas vérifiée au niveau réseau car elle le sera au niveau transport.
  - *Adresse source et Adresse destination* : ce sont des adresses IP.
  - *Options* : elles permettent, dans certains contextes, d'augmenter les contraintes d'acheminement du datagramme. Des bits de *Bourrage* complètent ce champ jusqu'à une taille fixe de 32 bits.
  - *Données* : de longueurs variables, elles ne peuvent cependant pas dépasser 65536 octets.

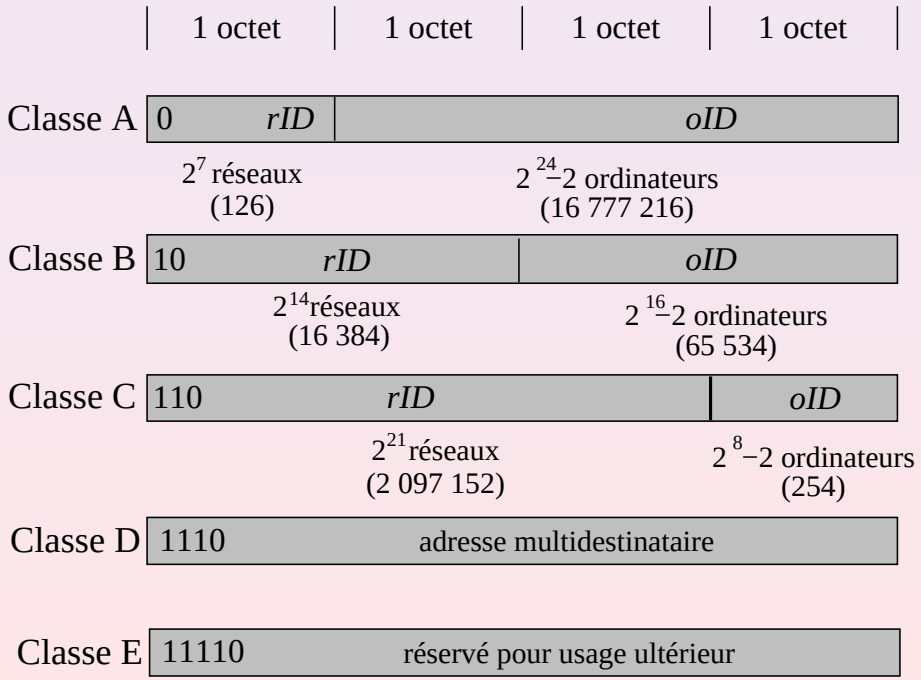
L'adressage IP

- Chaque élément du réseau allant du simple LAN au réseau Internet et travaillant avec le protocole IP doit posséder une adresse unique : son adresse IP.
- On attribue des adresses IP aux ordinateurs, aux routeurs, aux périphériques réseaux (imprimantes, caméras, copieurs, etc.).
- Une adresse IP est une suite de 32 bits regroupant l'identifiant réseau auquel appartient cet ordinateur (*rID*) et l'identifiant de ce dernier à l'intérieur du réseau (*oID*).
- Deux formes particulières d'adresses sont l'adresse réseau et son adresse de diffusion.

rID	*oID* tout à 0	adresse du réseau *rID*
rID	*oID* tout à 1	adresse de diffusion à tous les ordinateurs du réseau *rID*

Les classes d'adresse IP (1/2)

- Il existe cinq classes d'adresses IP notées classe A à classe E.
- On peut identifier la classe d'appartenance d'une adresse à partir de ses premiers bits.



Les classes d'adresse IP (2/2)

- Les classes A, B et C servent à adresser des réseaux de différentes tailles.
- Les classes A et B sont totalement saturées et plus aucune classe de ce type n'est disponible.
- La classe D définit des adresses multidestinataires correspondant à des groupes d'ordinateurs (adresses IP multicast).
- La classe E avait été prévue initialement pour les évolutions futures d'Internet. Dans les faits, elle a été très peu utile à cause de la saturation rapide des classes A, B et C.
- La forme binaire (chaîne de 32 bits) n'étant pas facile à mémoriser, on a l'habitude d'utiliser une forme décimale pointée du type $x_1.x_2.x_3.x_4$

Les différentes plages d'adresses IP

	Adresses théoriques		Adresses réellement disponibles	
Classe	**plus basses**	**plus hautes**	**plus basses**	**plus hautes**
A	0.0.0.1	127.255.255.254	0.1.0.1	126.0.0.0
B	128.0.0.1	191.255.255.254	128.0.0.1	191.255.0.0
C	192.0.0.1	223.255.255.254	192.0.0.1	223.255.255.0
D	224.0.0.1	239.255.255.254	224.0.0.1	239.255.255.254
E	240.0.0.1	247.255.255.254	240.0.0.1	247.255.255.254

- Les adresses dont le premier octet est 127 sont appelées adresses de rebouclage et désignent l'ordinateur local, quelques soient les valeurs des trois autres octets.
- Ces adresses sont utilisées pour les échanges de données entre les applications sur une même machine.
- Elles ne sont pas considérées comme des adresses de classe A.

Les masques de sous-réseaux

- On peut utiliser certains bits de l'identificateur (*oID*) pour découper le réseau en plusieurs sous-réseaux.
- Pour pouvoir interpréter une adresse IP, un ordinateur doit connaître le nombre de bits utilisés pour la partie *oID* dans un sous-réseau.
- On associe à chaque adresse un masque de sous-réseau exprimé sur 32 bits comme l'adresse IP.
- Chaque bit du masque qui correspond à l'adresse du réseau est positionné à 1 et chaque bit qui correspond à l'identifiant (numéro de machine) est positionné à 0.

Le routage IP : RIP (1/2)

- Le réseau Internet était basé au départ sur un routage à vecteur de distance mais au vu de sa forte croissance, il a été nécessaire d'en améliorer les techniques.
- Le protocole IP intègre toutes les fonctions nécessaires au routage au sein du protocole RIP (Routing Information Protocol).
- La technique porte le nom de routage par sauts successifs (Next-Hop Routing). Elle spécifie qu'un ordinateur ne connaît pas le chemin que va emprunter un datagramme mais seulement le routeur suivant à qui il va être transmis.
- Une table de routage contenant toutes les informations utiles est placée en mémoire dans l'élément actif (routeur ou ordinateur) quel que soit sa nature.

Le routage IP : RIP (2/2)

- Chaque ligne de la table contient trois champs :
  - une destination : adresse IP, adresse réseau ou la valeur *Default*.
  - le routeur de saut suivant : la passerelle. Il peut s'agir du routeur lui-même si le destinataire est situé sur un réseau directement accessible.
  - l'adresse de l'interface réseau à utiliser pour pouvoir accéder au routeur choisi.
  - la valeur du vecteur de distance : permet de connaître le nombre de sauts à effectuer avant d'atteindre le réseau abritant la machine distante.
- Les routeurs s'échangent les informations contenues dans leurs tables de routage au moyen de "messages RIP" à intervalles de temps régulier (généralement 30 sec.).

Les protocoles ARP et RARP

- Chaque interface réseau possède une adresse physique unique dépendante du type d'architecture (les adresses MAC sont différentes suivant la norme mise en place).
- L'adressage sur Internet est basé sur des adresses IP, de niveau réseau.

$\Rightarrow$ Il faut donc faire le lien entre les deux adresses (IP et MAC) d'une même machine : les protocoles ARP (Address Resolution Protocol) et RARP (Reverse Address Resolution Protocol)

- ARP permet de faire correspondre une adresse MAC à une adresse IP donnée et RARP permet l'inverse.

Le protocole ARP

- La résolution d'adresses est effectuée en trois étapes :
  1. Le protocole ARP émet un datagramme particulier par diffusion à toutes les stations du réseau et qui contient entre autre l'adresse IP à convertir.
  2. La station qui se reconnaît retourne un message (réponse ARP) à l'émetteur avec son adresse MAC.
  3. L'émetteur dispose alors de l'adresse physique du destinataire et ainsi la couche liaison de données peut émettre les trames directement vers cette adresse physique.
- Les adresses résolues sont placées dans un cache ce qui évite de déclencher plusieurs requêtes lorsque plusieurs datagrammes doivent être envoyés.

Couche transport (niveau 4)

- La première des couches du modèle OSI qui n'est pas présente sur les éléments intermédiaires de type routeur.
- Améliorer la fiabilité des transmissions de niveau réseau de l'émetteur au récepteur.
- Des services similaires à ceux fournis par la couche réseau, complétés par des fonctions de contrôle de qualité et d'amélioration de celle-ci.
- Ces services peuvent être orientés connexion ou pas mais une meilleure fiabilité est obtenue en mode connecté.

Gestion d'une connexion (1/3)

- Identification des extrémités :
  - Mise en place d'un canal de transmission entre la station émettrice et le destinataire.
  - L'identification au moyen de son adresse IP n'est pas nécessaire pour une machine car plusieurs s'exécutent souvent en parallèle sur une même machine.
  - L'identification se fera donc au moyen d'une adresse IP et d'un numéro de port associé à l'application.
- Établissement d'une connexion :
  - On appelle TPDU (Transport Protocol Data Unit) les entités envoyées par une couche transport à ses homologues.
  - Des primitives de niveau transport permettent aux TPDU de réaliser des actions (connexion, envoi de données, réception, déconnexion, etc.).

Gestion d'une connexion (2/3)

- Établissement d'une connexion (suite) :
  - Deux datagrammes partant d'un même émetteur vers un même récepteur peuvent emprunter des chemins différents.
  - Certains nœuds du réseau peuvent dupliquer l'information.
  - Une demande connexion de niveau transport pourrait donc entraîner plusieurs demandes de connexion de niveau réseau.

  $\Rightarrow$ Identification des TPDU transmises lors de la phase de connexion.
  - Trois étapes pour la mise en place d'une connexion au niveau transport :
    1. L'émetteur envoie une TPDU *CONNECT.request* permettant au récepteur de s'identifier.
    2. Le récepteur renvoie une réponse *CONNECT.response* avec son identifiant.
    3. L'émetteur peut alors envoyer des données tout en accusant réception de la réponse.

Gestion d'une connexion (3/3)

- Transmission des données :
  - Une TPDU *DATA.request* permet d'initier une demande de données ou de demander à un émetteur de retransmettre des données qui seraient parvenues erronées au récepteur.
  - Les données demandées sont transmises par une TPDU *DATA.indication*.
- La phase de déconnexion est réalisée en trois étapes :
  - Lorsque l'une des deux extrémités souhaite se déconnecter, elle envoie une demande de déconnexion (TPDU *DISCONNECT.request*).
  - L'autre extrémité peut alors ignorer la requête. Dans le cas contraire, elle envoie son accord (TPDU *DISCONNECT.request*).
  - L'initiateur de la demande de déconnexion signale alors sa déconnexion par une TPDU *DISCONNECT.indication* puis interrompt effectivement la communication.

Qualité de service

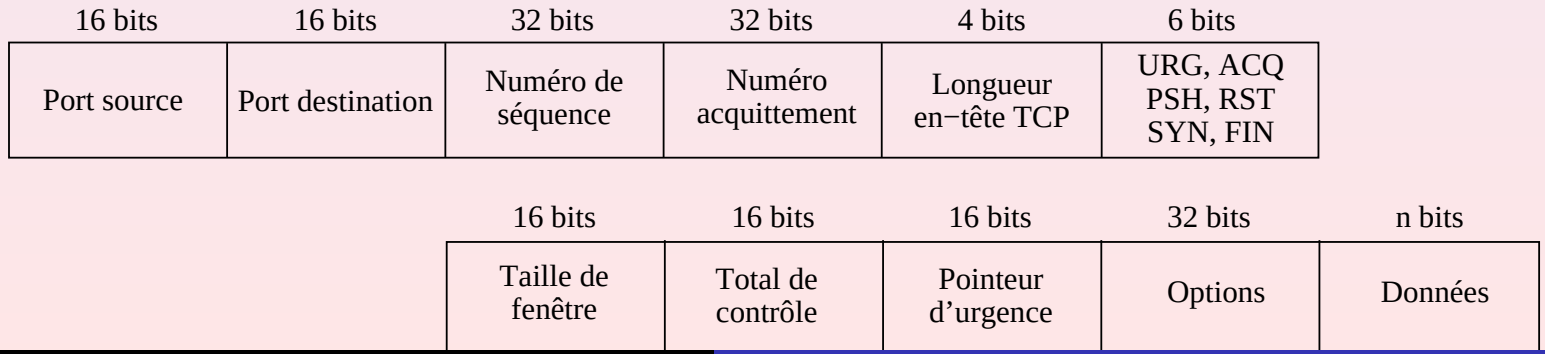
- Des critères permettant de fixer des exigences pour les communications permettront d'interrompre à tout moment une communication s'ils ne sont pas respectés.
- Quelques exemples de contrôle de qualité :
  - Temps d'établissement de la connexion.
  - Débit de liaison : nombre d'octets utiles qui peuvent être transmis par secondes.
  - Protection : possibilité pour l'utilisateur d'interdire à un terminal tiers l'intrusion sur sa ligne pour lire ou modifier les données transmises.
  - Taux d'erreur résiduel : rapport entre le nombre de messages perdus ou mal transmis et le nombre total de messages transmis sur une période donnée.

Protocoles TCP, UDP, ICMP (1/5)

- Le protocole TCP : Transmission Control Protocol.
  - L'un des plus répandu au niveau transport.
  - La plupart du temps associé à IP (TCP/IP) pour améliorer la qualité de service.
  - Orienté connexion, il rend fiable la transmission des données entre les applications réseaux.
  - Il offre un certain nombre de services :
    - ouverture et fermeture de connexion,
    - découpage des données en entités appropriées à la constitution de datagrammes,
    - contrôle de la qualité de service,
    - gestion des problèmes de transmission et reprise en cas d'interruption,
    - multiplexage amont.

Protocoles TCP, UDP, ICMP (2/5)

- Le protocole TCP (suite)
  - Le format des TPDU utilisées par TCP est le suivant :
    - Le *Port source* et le *Port destination*.
    - Le *Numéro de séquence* qui spécifie l'emplacement du segment TCP après le découpage de l'entité de niveau supérieur.
    - L'acquittement des segments reçus effectué par un *Numéro d'acquittement* dans la réponse renvoyée à l'émetteur.
    - La *Longueur de l'en-tête TCP* pour connaître le début des données.
    - Six bits particuliers (UGR : TPDU prioritaire, ACQ : acquittement, RST : refus d'une TPDU, SYN : connexion en cours d'ouverture, FIN : fermeture de la connexion) précisent la nature de la TPDU.



Protocoles TCP, UDP, ICMP (3/5)

- Le protocole UDP : User Data Protocol.
  - Un fonctionnement très proche de IP : reprends la plupart de ses fonctions et lui octroie plus de fiabilité.
  - UDP est similaire à TCP mais fonctionne en mode non connecté.
  - Un segment UDP est constitué de 5 champs :
    - Un *Port source* et un *Port destination* similaire à ceux de TCP.
    - Le champs contenant les *Données* de longueur variable, le champ *Longueur totale*, le contrôle d'erreur (champs Total de contrôle).

16 bits	16 bits	16 bits	16 bits	n bits
Port source	Port destination	Longueur totale	Total de contrôle	Données

Protocoles TCP, UDP, ICMP (4/5)

- Le protocole ICMP : Internet Control Message Protocol.
  - IP est non fiable $\Rightarrow$ nécessité de vérifier le bon acheminement des données.
  - Protocole de notification d'erreurs conçu pour la diffusion d'informations d'administration sur Internet.
  - Deux catégories de messages dans ICMP : les messages d'erreur et les messages d'administration.
  - ICMP est indispensable au bon fonctionnement des couches réseaux et transport du modèle TCP/IP (IP, TCP et UDP) car il informe des erreurs survenues telles que :
    - destination inaccessible,
    - port inaccessible,
    - corruption de messages.

Protocoles TCP, UDP, ICMP (5/5)

- Le protocole ICMP (suite).
  - ICMP = un protocole d'administration du réseau :
    - échange d'informations concernant le routage,
    - annonce et gestion des masques réseaux,
    - vérification de l'accessibilité,
    - gestion de l'heure,
    - aide au contrôle de congestion.
  - ICMP est implémenté au sein des programmes *ping*, *traceroute*.

Couche session (niveau 5)

- Objectif : fournir un ensemble de services pour la coordination des applications.
- Unité d'échanges : le datagramme.
- Point de vue : processus/services, applications.
- Elle offre des services de synchronisation élémentaire pour organiser le dialogue et la reprise sur erreur d'une transaction distribuée :
  - donner la parole à tour de rôle aux différents membres d'une connexion.
  - définir des points de reprise dans un flot d'échanges.
  - garantir la fin cohérente d'une communication.

Couche présentation (niveau 6)

- Objectifs :
  - permettre de manipuler des objets typés plutôt que des bits,
  - fournir une représentation standard pour ces objets quelques soient les architectures de matériel, de langages utilisés, etc.
- Unité d'échanges : le datagramme.
- Services :
  - définition d'une notation abstraite pour les objets typés.
  - compression, cryptage.

Couche application (niveau 7)

- Elle permet de mettre en œuvre un certain nombre d'applications réseaux généralement basées sur des protocoles de niveau application. Il s'agit notamment :
  - des méthodes de communication telles que la messagerie électronique ou les canaux de communication,
  - du transfert de fichier au travers du protocole FTP,
  - de la prise de commande à distance permettant notamment l'administration distante des systèmes d'information répartis,
  - du *World Wide Web* basé sur le protocole HTTP,
  - des outils liés directement à l'administration des réseaux (Ping, SNMP, ...),
  - de la sécurisation des transmissions au travers du protocole SSL.

Les méthodes de communication (1/4)

- SMTP : le courrier électronique
  - l'application la plus rencontrée dans les réseaux,
  - elle permet l'envoi de texte ou de fichiers à un destinataire ou groupe de destinataires,
  - l'envoi se fait en mode non connecté, pas de nécessité que la boîte au lettre du récepteur soit disponible ou même qu'elle existe,
  - les adresses électroniques :
    - chaque utilisateur possède une adresse propre,
    - son format est le suivant : `[nom]@[machine].[site].[pays]`
    - le champ `[site]` trouve son origine dans l'organisation des universités au début de l'Internet : généralement plus renseigné à l'heure actuelle. Les adresses des particuliers font référence aux fournisseurs d'accès Internet (FAI). La forme des adresses courantes devient alors `[nom]@[FAI].[pays]`.
    - le pays est identifié par deux lettres (fr), normalisées par l'ISO.

Les méthodes de communication (2/4)

- Le protocole SMTP (Simple Mail Transfert Protocol) :
  - présent sur la couche application du modèle TCP/IP,
  - protocole de gestion du courrier électronique,
  - l'envoi et la réception des messages se fait au moyen d'une connexion TCP,
  - avant de transmettre un message, un client doit s'assurer de l'existence de la boîte aux lettres sur le serveur,
  - le démon SMTP écoute sur un port donné pour détecter l'arrivée de nouveaux messages,
  - le protocole SMTP nécessite que les machines (serveurs) restent connectées au réseau en permanence.

Les méthodes de communication (3/4)

- Le protocole POP3 (Post Office Protocol) :
  - problème : les machines des particuliers ne sont pas connectées au réseau en permanence,
  - le stockage des messages se fait au niveau des FAI,
  - POP3 permet de télécharger son courrier depuis un serveur distant.
- Les nouvelles (news) et le protocole NNTP (News Network Transfert Protocol) :
  - Les *newsgroup* sont des sites auxquels les utilisateurs intéressés par un même thème peuvent se connecter.
  - Ce protocole est basé sur une inscription des utilisateurs.
  - La transmission des données entre les différents serveurs de news se fait au moyen du protocole NNTP.
  - Basé sur TCP, il fonctionne en mode connecté et utilise le port 119.

Les méthodes de communication (4/4)

- Le protocole NNTP (News Network Transfert Protocol) :
  - Mise à jour, en cas de modifications, d'ajouts ou de suppressions d'une information sur un serveur, la base de données des autres serveurs.
  - Un serveur ne transmet pas les informations dont il est dépositaire à tous les autres serveurs mais uniquement à ceux qu'il connaît directement et ces serveurs peuvent à leur tour retransmettre ces informations.
  - Permet à un utilisateur connecté au forum de discussion de déposer des données sur un serveur à partir d'un poste de travail quelconque du réseau.

FTP : le transfert de fichiers

- FTP fait partie de la pile des protocoles TCP/IP.
- Il permet aux utilisateurs :
  - de se connecter à un serveur FTP puis de se déconnecter lorsque le téléchargement est terminé.
  - de transférer des fichiers, quel que soit leur nature, entre les deux extrémités de la connexion et dans les deux sens.
- L'accès se fait avec un login et un mot de passe. Lorsque l'accès se fait en mode anonyme (anonymous), le mot de passe demandé est une adresse Internet.

TELNET : la prise de commande à distance

- TELNET est un protocole de niveau application du modèle TCP/IP.
- Fonctionne en mode connecté (TCP) sur le port 23.
- Une connexion TELNET se fait en deux phases :
  - une phase d'authentification.
  - une phase de travail à distance.
- Plusieurs programmes sont basés sont l'utilisation de ce protocole :
  - *telnet* qui est l'utilitaire de prise de commandes à distance qui offre un éventail de fonctionnalités permettant l'exécution interactive de commandes dans l'environnement distant.
  - *rlogin*, similaire à *telnet*, la demande d'authentification n'est pas effectuée si l'identifiant d'accès est le même aux deux extrémités.
  - *rsh* permet d'exécuter des commandes shell dans l'environnement propre au système d'exploitation distant.

DHCP : Dynamic Host Configuration Protocol (1/2)

- Pourquoi ? Faciliter la gestion des adresses de machines dans les réseaux de grandes tailles qui se modifient souvent.
- DHCP :
  - Attribuer automatiquement une adresse IP à une machine qui se connecte au réseau.
  - Plusieurs phases :
    1. Le client envoie un message d'exploration DHCPDISCOVER dans un paquet sur l'adresse de broadcast 255.255.255.255.
    2. Si un serveur DHCP reçoit un tel message, il y répond pour signaler qu'il est disponible.
    3. Le serveur consulte sa base pour savoir si l'adresse physique du client ne correspond pas à une adresse IP fixe. Si ce n'est pas le cas il choisit une adresse IP disponible et l'envoi au client.

DHCP : Dynamic Host Configuration Protocol (2/2)

- Validité des adresses dynamiques :
  - Pour une période limitée appelée *bail*.
  - À la moitié du bail, le client envoie une requête au serveur pour demander la prolongation du *bail*. S'il n'a pas de réponse ou que le serveur refuse, il continue d'utiliser l'adresse pendant la moitié du temps restant puis envoi une nouvelle requête.
  - À l'expiration du bail, si le client n'a pas obtenu de prolongation, il doit abandonner l'adresse.
  - Pour éviter les pics de trafic qui pourraient survenir lors du démarrage d'un grand nombre de machines, les requêtes DHCP sont envoyées à intervalles de temps aléatoires.
  - Certaines informations sont stockées chez le client ce qui évite de redemander ces informations lors du redémarrage.

DNS : Domain Name System

- Faire correspondre un nom (facile à retenir) à une adresse IP ou MAC qui est une suite de chiffres.
- Structure des DNS :
  - Distribution des informations sur de multiples DNS.
  - Un DNS est à la fois client et serveur.
  - Basé sur une structure hiérarchique en haut de laquelle sont situés des serveurs ROOT (Il en existe 13 pour l'ensemble de l'Internet).
  - Envoi de requêtes de types récursives.
  - Un nom DNS est composé d'une suite de caractères alphanumériques séparés par des points.
  - La structure des enregistrements d'une base DNS suit le standard BIND (*Berkeley Internet Domain Name*).