Université Internationale de Casablanca

LAUREATE INTERNATIONAL UNIVERSITIES

Réseaux informatiques

Dr Mohammed BOUTABIA

Université Internationale de Casablanca

Qu’est ce qu’un réseau?

- Un réseau est un ensemble de nœuds reliés par des liens
- Ex: réseau autoroutier, réseau électrique, réseau téléphonique, réseau informatique
- Le rôle principale d’un réseau est de relier => trouver un chemin d’un point de départ à un point d’arriver

Réseaux informatiques

- Ensemble d'ordinateurs (nœuds) reliés entre eux avec des supports de transmission (lien)
- Exemples: réseau d'entreprise, internet, réseaux 3G…
- Les ordinateurs s'échangent des informations => l'information doit trouver un chemin depuis une source à une destination

Pourquoi un réseau informatique?

- Les utilisateurs cherchent toujours un service (une application):
  - Se connecter à un site web
  - Envoyer un email
  - Télécharger des fichiers
  - Imprimer un document sur une imprimante réseau
- Deux objectifs principaux: Partage de ressource et communication
- Deux modèles ou architectures: client/serveur versus peer to peer

Partage de ressources

- le partage de fichiers : les données circulent par un câble et non par des supports de stockage (disquettes, clefs USB).
- Tous les ordinateurs du réseau peuvent accéder aux mêmes données et les modifier.
- le partage de ressources matérielles : imprimante, modem, disque dur, lecteur CD…
- le partage des applications : travail dans un environnement Multiutilisateurs.
- la garantie de l'unicité de l'information (base de données)

La communication

- la communication entre personnes (courrier électronique, messagerie instantanée, …)
- Téléphonie
- Distraction: jeu en réseau
- Vidéoconférence, TV personnel
- Réseaux sociaux: facebook, twitter

Architecture client serveur

- Un serveur fournis un service à un ou plusieurs clients
- La majorité des services sur les réseaux (y compris internet) suivent ce modèle
- Maitrisable par les fournisseurs de service
- Doit être dimensionné selon la demande

Avantage de la centralisation

- simplifier la maintenance des logiciels (mise à jour plus facile lors du changement de version).
- libérer de l'espace disque sur les postes de travail.
- Gestion d'accès centralisée

inconvénient

- vulnérabilité de la machine abritant les ressources. One point failure => si cette machine tombe en panne tout le système s'arrête
- Matériel sophistiqué est cher pour les serveurs
- Diminution de performance aux moments des rush

Architecture peer to peer

- Architecture distribuée (pas de serveur)
- Tous les nœuds sont à pied d'égalité
- Peuvent fournir le service ou le solliciter (télécharger un fichier d'un pair et envoyer un autre fichier à un autre pair)
- chaque nœud est client et serveur en même temps
- Architecture non maitrisable par une entité particulière=> partage illicite de document

Avantage inconvenant

- Avantages= inconvénients client/serveur
- Inconvénients = avantages client/serveur

Les types de données

- Le texte: web, fichiers (PDF, Word, ppt…)
- La voix: Skye, SIP
- Les images: photo, bannières
- Les vidéos: vidéo streaming, IPTV
- Le réseau doit tenir en compte des contraintes de chaque types de données
  - la vidéo peut tolérer des erreurs mais pas le texte
  - Le texte peut tolérer le retard mais pas la vidéo

Conversion des données

- Tout type de donnée est sous forme numérique
- Comment transmettre l'information au format binaire (0111010101000)?
- Passage par une conversion selon le type du média (support) utilisé
- électrique avec un câble en cuivre=> 0=0v, 1=5v
- optique sur des fibres optique=> 0=obscurité, 1=lumière

Catégories de réseaux

- Catégories de réseaux basées sur leur étendue géographique :
  - PAN
  - LAN
  - MAN
  - WAN

Réseaux personnels
Personal area networks

- Réseaux de petit étendue qui fonctionnent autour d'une personne
- portée de quelques mètres
- Exemples: câble USB, Bluetooth, infra rouge

Réseaux locaux
local area networks

- Il s'agit un ensemble d'ordinateurs appartenant à une même organisation et reliés entre eux dans une petite aire géographique par un réseau, souvent à l'aide d'une même technologie
- L'étendue est de quelques centaines de mètres
- Exemples: Ethernet, Wifi

Réseaux métropolitains
metropolitain area network

- Un réseau composé de plusieurs d'ordinateurs sur un campus ou une ville
- Exemples: Ethernet métropolitains, wimax

Réseaux étendus
wide area networks

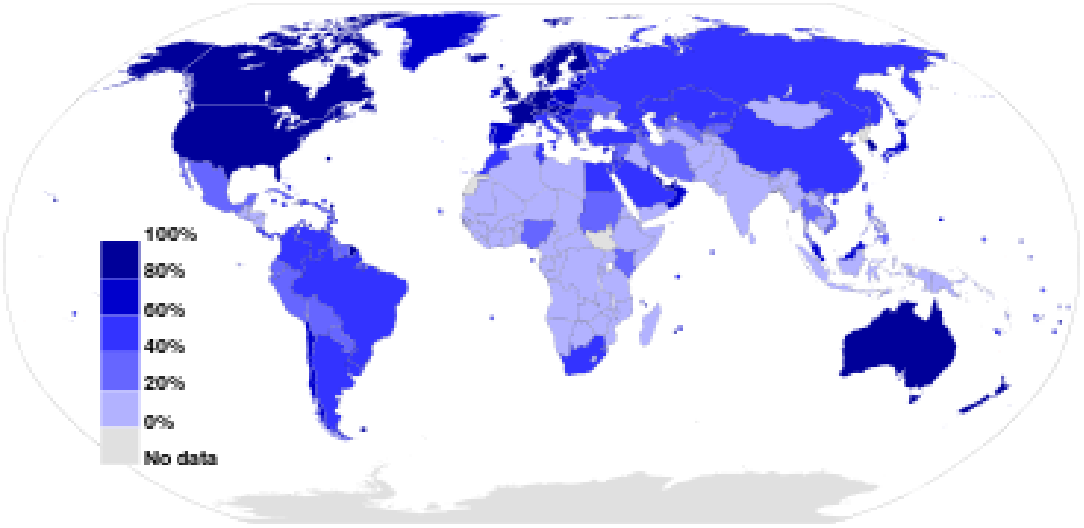
- Un réseau informatique couvrant une grande zone géographique (à l'échelle d'un pays ou transfrontières)
- Exemple: fibre optique transatlantique, satellite

débit

- Le débit d'une ligne est la quantité d'information envoyée par seconde
- Unité: bit/s
- Vitesse ou débit?
- Vitesse de transmission est la vitesse avec laquelle une carte réseau peut mettre les bit sur le support
- La Vitesse de propagation est la longueur (m) parcouru par les signaux (informations) dans le support (lien) par seconde ≈ 273000km/s (dans le cuivre)
- Le débit varie selon le support utilisé

Internet

- Un réseau informatique qui relie plusieurs réseaux => le réseau des réseaux
- Réseau international
- Englobe des millions d'ordinateurs 2,9 milliards en 2014
- pourcentage d'internautes par pays 2012:



Types de fournisseurs

- Fournisseur d'accès : se chargent du transport des données
  - ex: Maroc Telecom)
- Fournisseur de service: fourni un service particulier
  - ex: service de messagerie instantané, IPTV…
- Fournisseur de contenu: fournie les données qui sont utiles à l'utilisateur
  - ex : producteur de film, librairie électronique

Cout d’un réseau

- Ce que coûte un réseau:
  - l'installation : coût des équipements et mise en place
  - l'entretien, l’administration et fonctionnement (électricité basse tension)

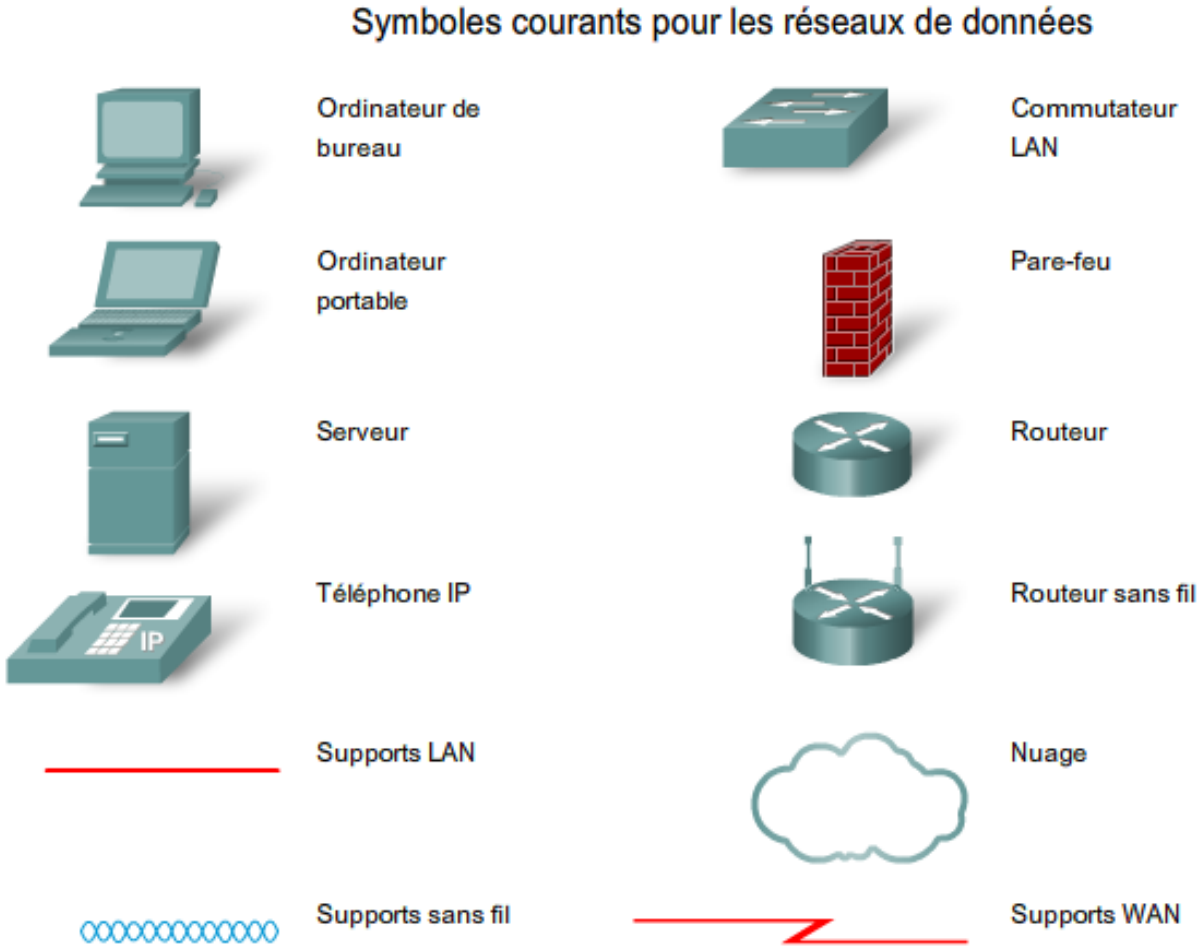
⇒ ne coûte rien à long terme !

  - les équipements coûtent le même prix, qu'on les utilise ou pas
  - Mode de payement: à la durée, à la quantité d’informations envoyées, forfaitaire (illimité)
  - Voie sur IP gratuit => même à l’international (free, neuf, Bouygues…)

Composants d’un réseau

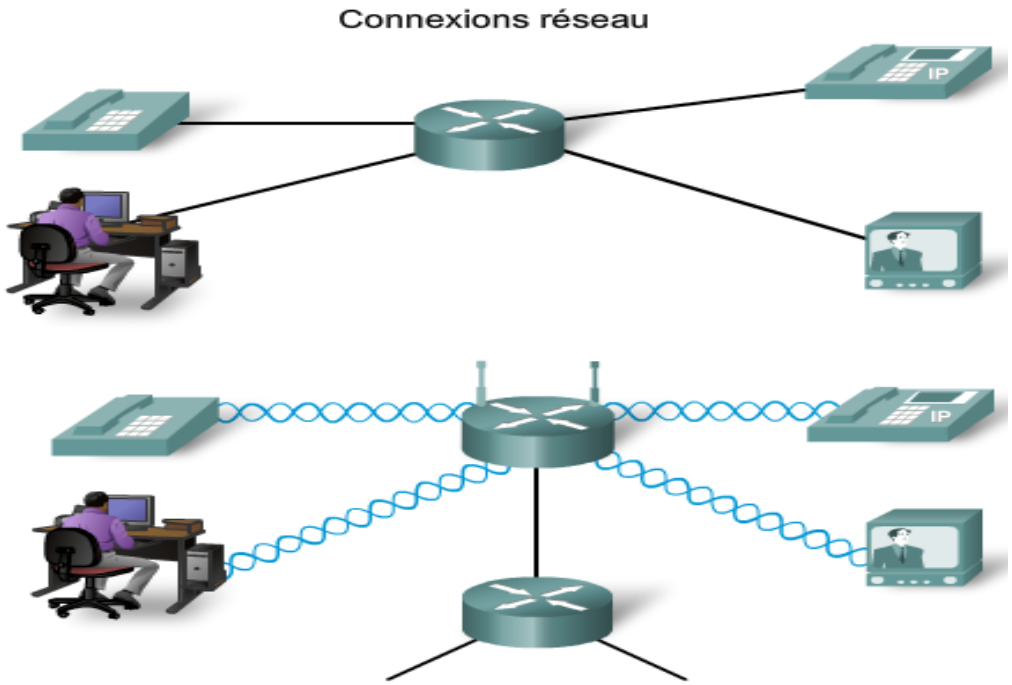
- Support
- Périphériques
- Message
- Les protocoles

symboles


Symboles courants pour les réseaux de données
Ordinateur de bureau
Ordinateur portable
Serveur
Téléphone IP
IP
Supports LAN
Supports sans fil
Commutateur LAN
Pare-feu
Routeur
Routeur sans fil
Nuage
Supports WAN

Support

- câble en cuivre (paires en cuivre torsadées, câble coaxiale, câble série)
- Fibre optique
- Faisceaux hertziens (infra rouge, radio, wifi)



périphériques

- Périphérique d'extrémité ou terminaux: PC, serveur, tablette, téléphone mobile…
- Périphérique d'interconnexion: hub, Switch, routeur, firewall…

Protocoles

- Un protocole est l'ensemble des règles qui permettent à deux machines de communiquer (se comprendre)
- Les suites de protocoles réseau décrivent des processus tels que :
  - le format ou la structure du message ;
  - la méthode selon laquelle des périphériques réseau partagent des informations sur des chemins avec d'autres réseaux ;
  - comment et à quel moment des messages d'erreur et système sont transférés entre des périphériques ;
  - la configuration et l'arrêt des sessions de transfert de données.

Exemple de protocoles

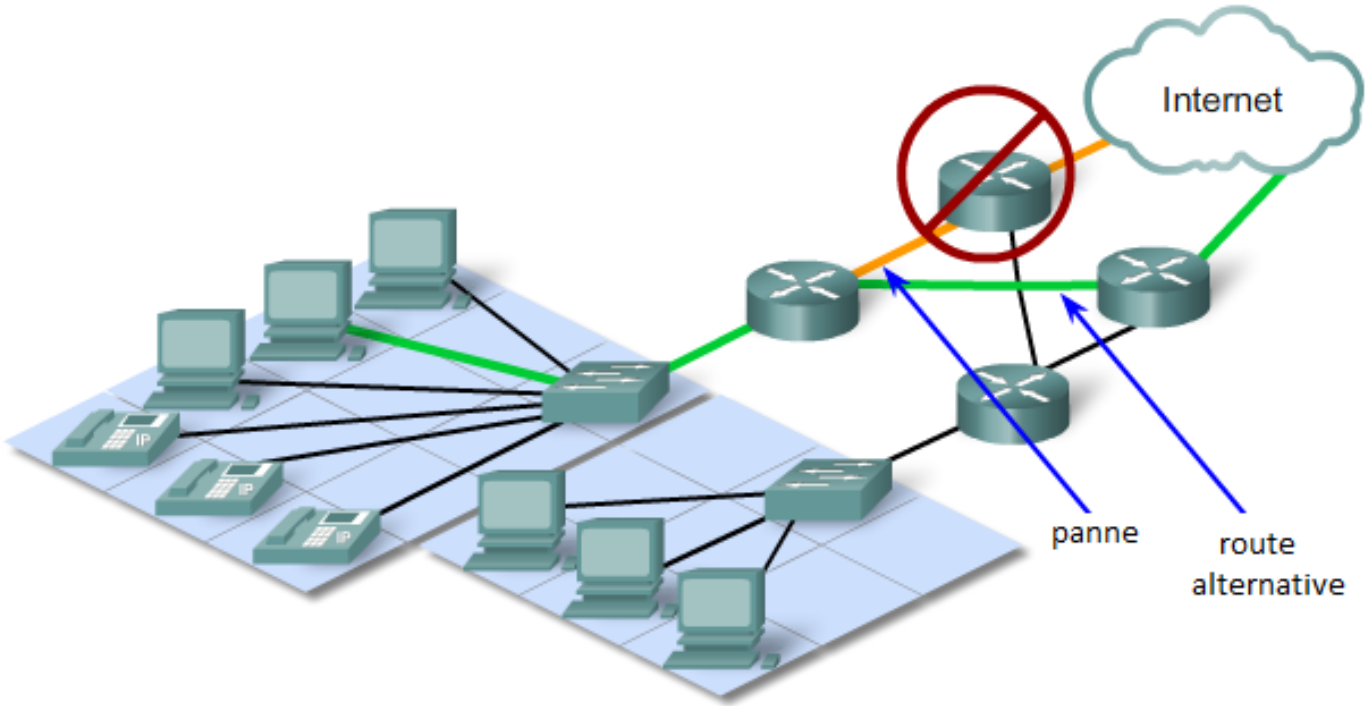
Service	Protocole (« Règle »)
World Wide Web (WWW)	HTTP (Hypertext Transport Protocol)
Courriel	SMTP (Simple Mail Transport Protocol) POP (Post Office Protocol)
Message instantané (Jabber, AIM)	XMPP (Extensible Messaging and Presence Protocol) OSCAR (Open System for Communication in Realtime)
Téléphonie sur IP	SIP (Session Initiation Protocol)

Caractéristiques d’un réseau

- Tolérance aux pannes
- Évolutivité
- Qualité de service
- sécurité

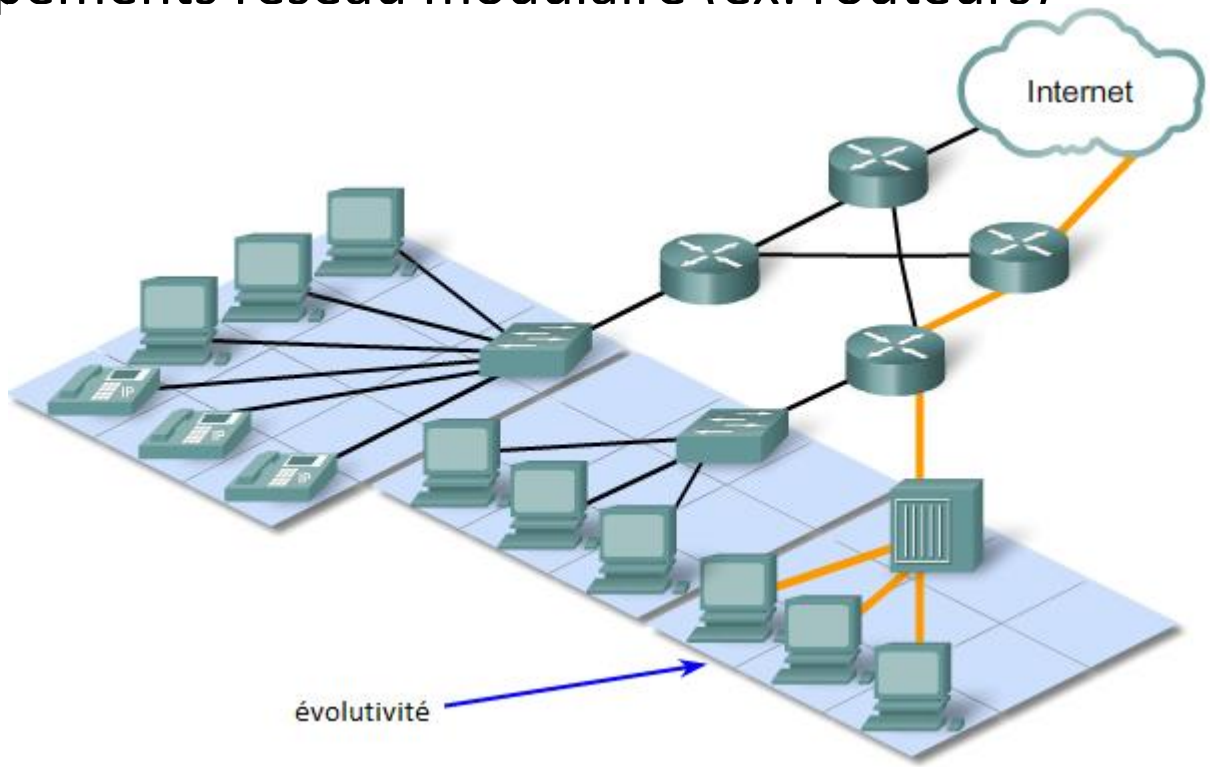
Tolérance aux pannes

- Un réseau doit être tolèrent aux pannes
- Les paquets doivent trouver une route alternative
- Lignes de backup
- Réseau maillé au niveau du cœur



évolutivité

- Un réseau doit pouvoir s'étendre sur de nouvelles stations ou réseaux
- Cette extension ne doit pas affecter sans dégradation des performances au niveau utilisateur
- Équipements réseau modulaire (ex: routeurs)



Qualité de service

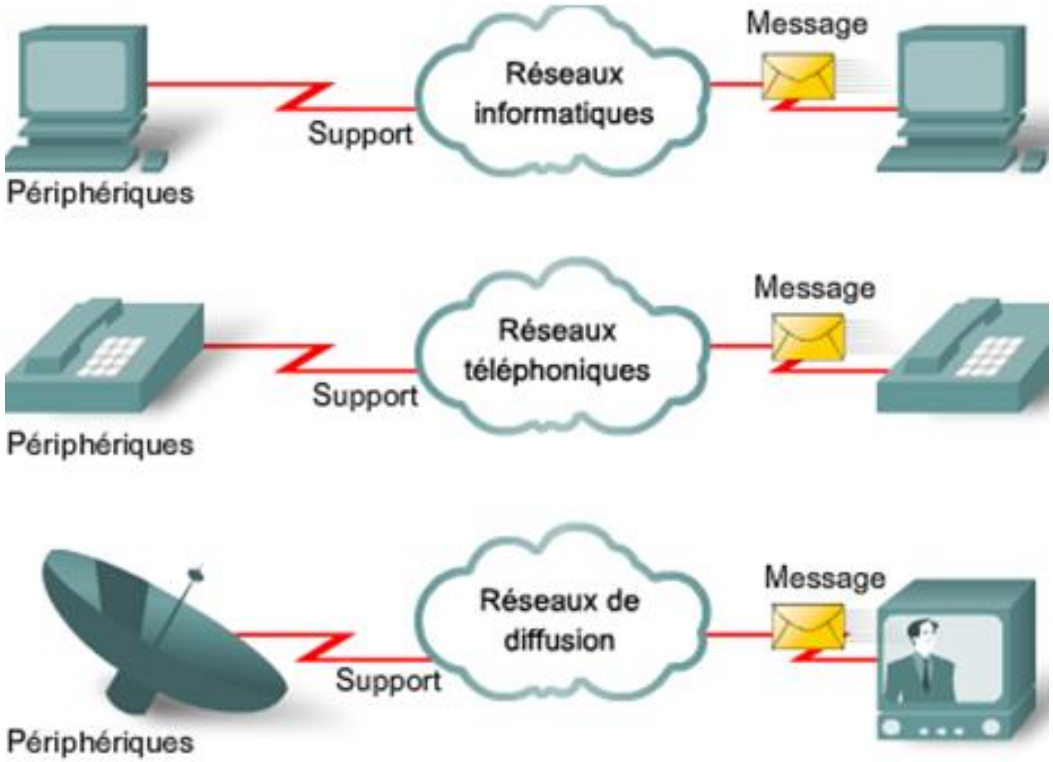
- Un service doit être assuré avec un minimum de QoS requis
- Les différent services n’ont pas besoin du même niveau de la QoS => priorisation
- Contrainte sur la bande passante disponible, délai de bout en bout et taux de perte

sécurité

- Protéger l’accès aux ressources réseaux par des personnes non autorisés
- Assurer la confidentialité des données sur internet
- Mettre une politique de sécurité au sain de l’entreprise

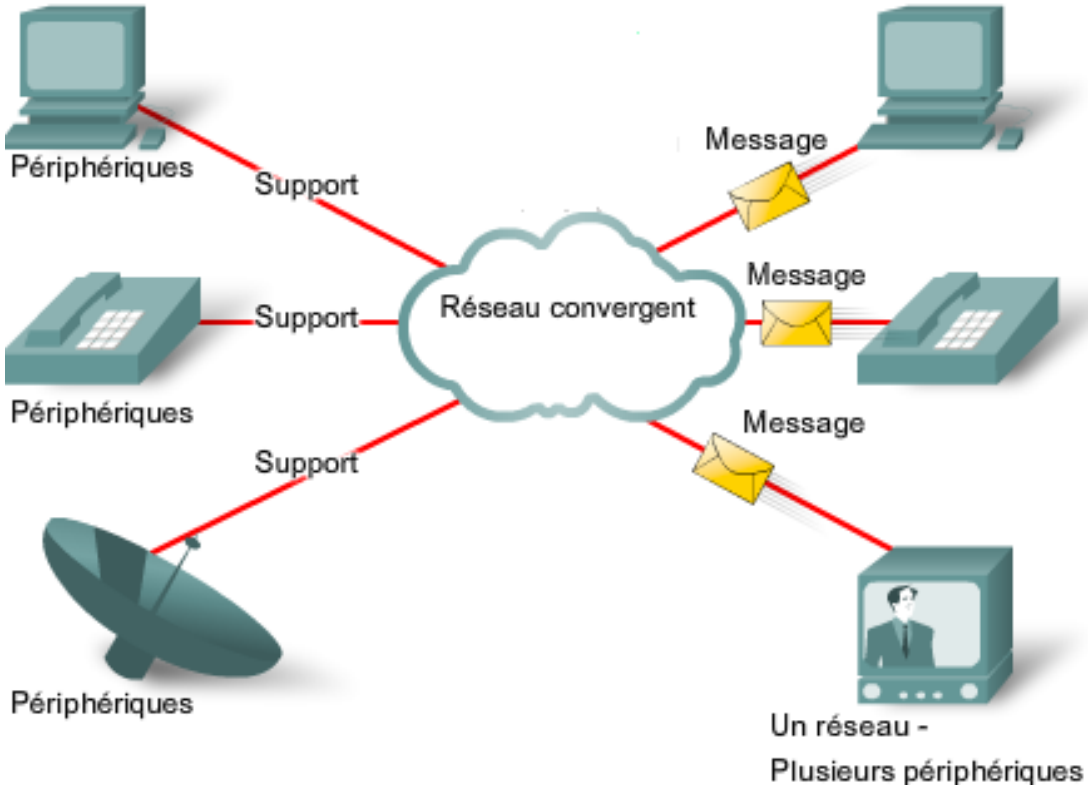
Un réseau par service

- Chaque réseau est dédié pour un service particulier
- Multitude de réseau physique
- Ressources non optimisées



convergence

- Un même réseau pour plusieurs services
- Optimisation des ressources
- Exemple: triple Play

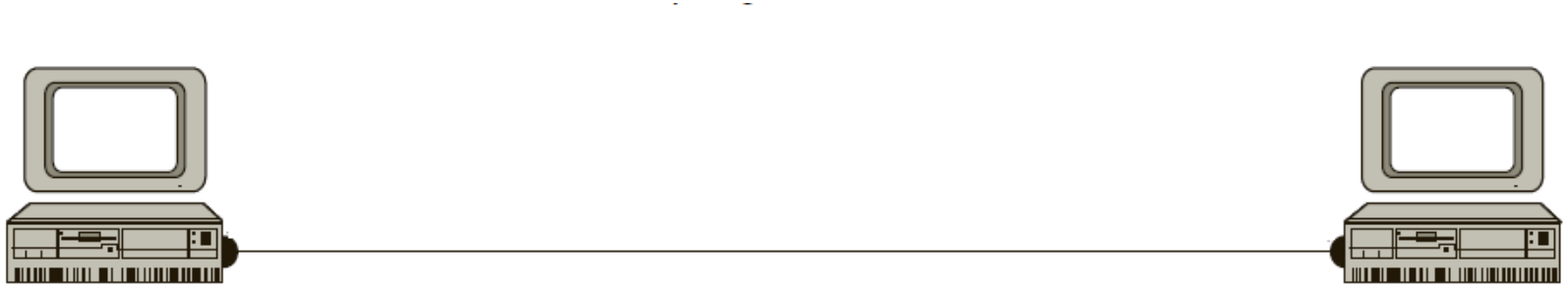


topologies

- Physique: topologie de branchement des fils
- Logique: chemin suivi par les informations (les trames)
- Topologies des réseaux:
  - Point à point
  - Bus
  - Anneau
  - Étoile
  - maillée

Point à point

- Les données sont envoyées directement vers la destination (pas besoin d'adressage) soit en full duplex ou half duplex
- exemple: liaison série



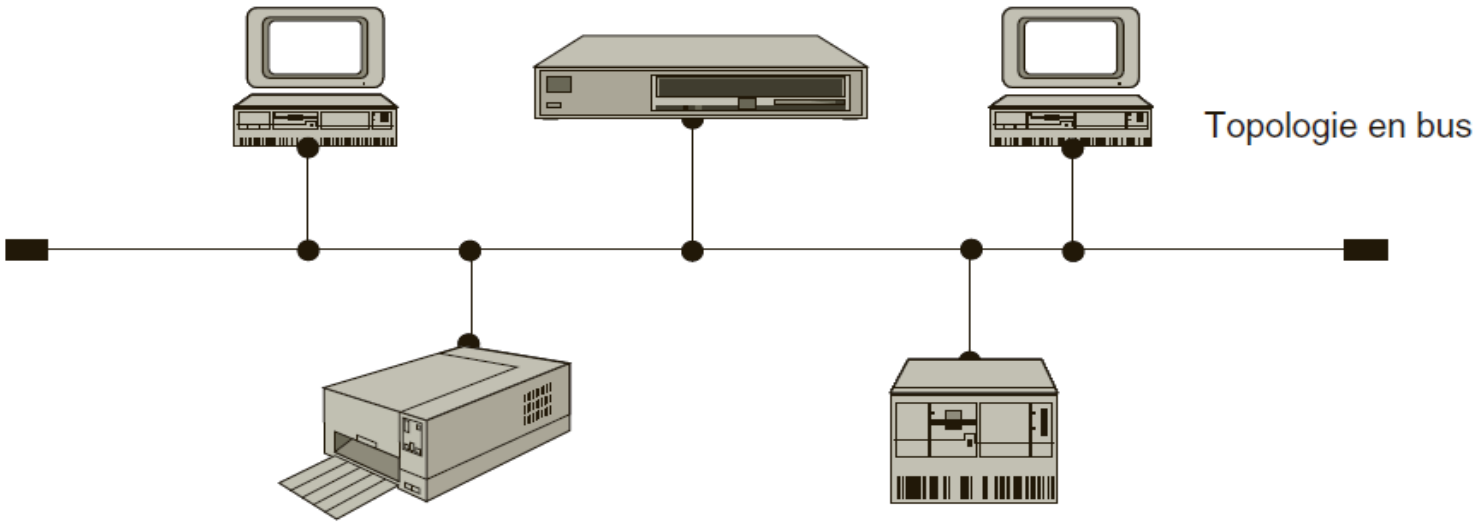
Liaison point à point.

Half duplex/full duplex

- Half duplex (unidirectionnel): une machine transmet à la fois => besoin de synchronisation au préalable (ex: radio police)
- Full duplex (bidirectionnel): les deux machines peuvent transmettre en même temps (ex: téléphone RTC)

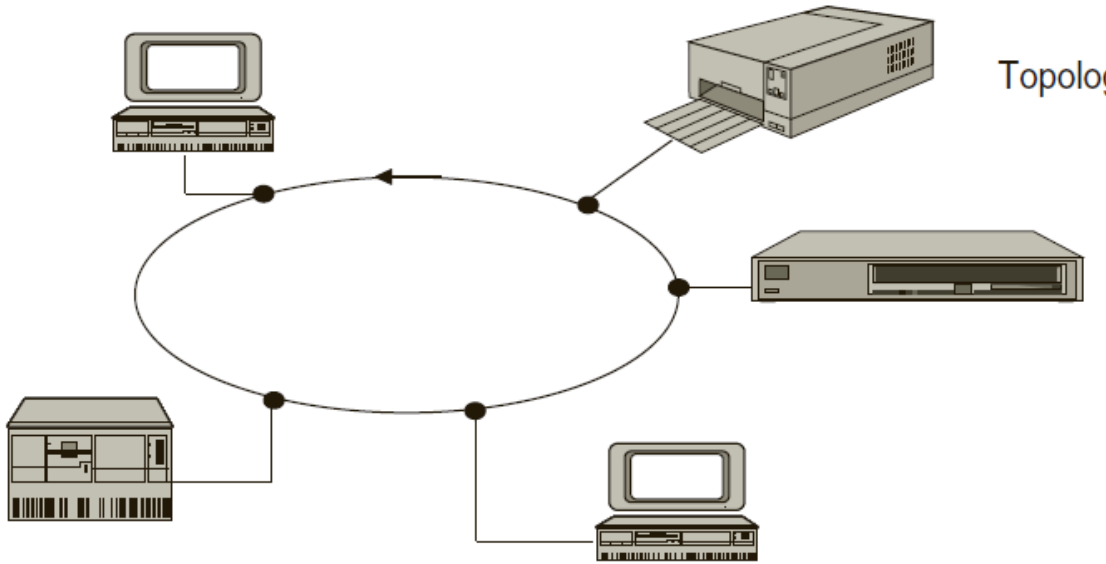
bus

- les trames sont diffusées sur tout le réseau (réseau à diffusion)
- chaque station accède directement au réseau
- exemple: réseau Ethernet



anneau

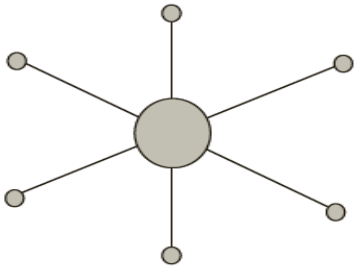
- chaque station est connectée à la suivante par une liaison point à point.
- Les messages circulent, dans un seul sens sur l'anneau.
- Chaque station reçoit le message. Si le message lui est destiné alors la station recopie celui-ci et le régénère, sinon la station se contente de le régénérer (grandes distances)
- sensible à la rupture de l'anneau.

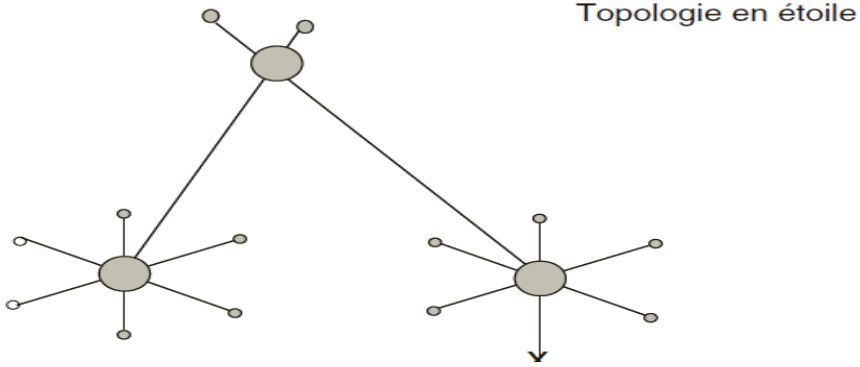


Topologie en anneau

Etoile

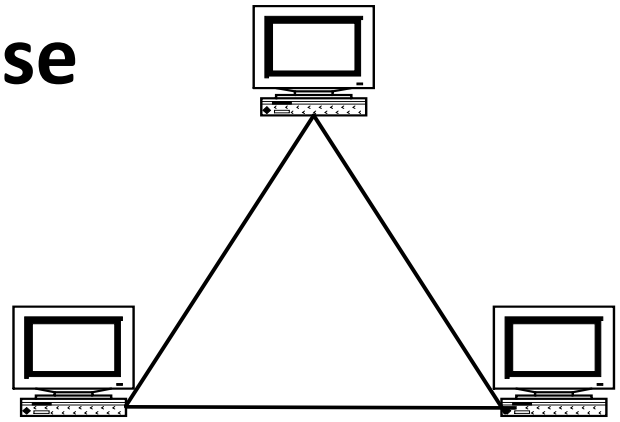
- tous les messages transitent par le point central de l'étoile qui joue le rôle de concentrateur.
- Le concentrateur est un composant actif qui examine tous les messages et les retransmet au bon destinataire.
- Si l'un des câbles se rompt, seul l'ordinateur relié au câble est affecté
- si le concentrateur tombe en panne, l'ensemble des ordinateurs ne peuvent plus communiquer => one point failure





Topologie maillée

- Chaque ordinateur est relié à chacun des autres par un câble séparé.
- tolérance aux pannes=> Lorsqu'un câble devient inopérant, il existe d'autres itinéraires d'acheminement des données.
- Utilisé dans les réseaux cœurs des opérateurs
- **=> Topologie très coûteuse**



Modèle en couche

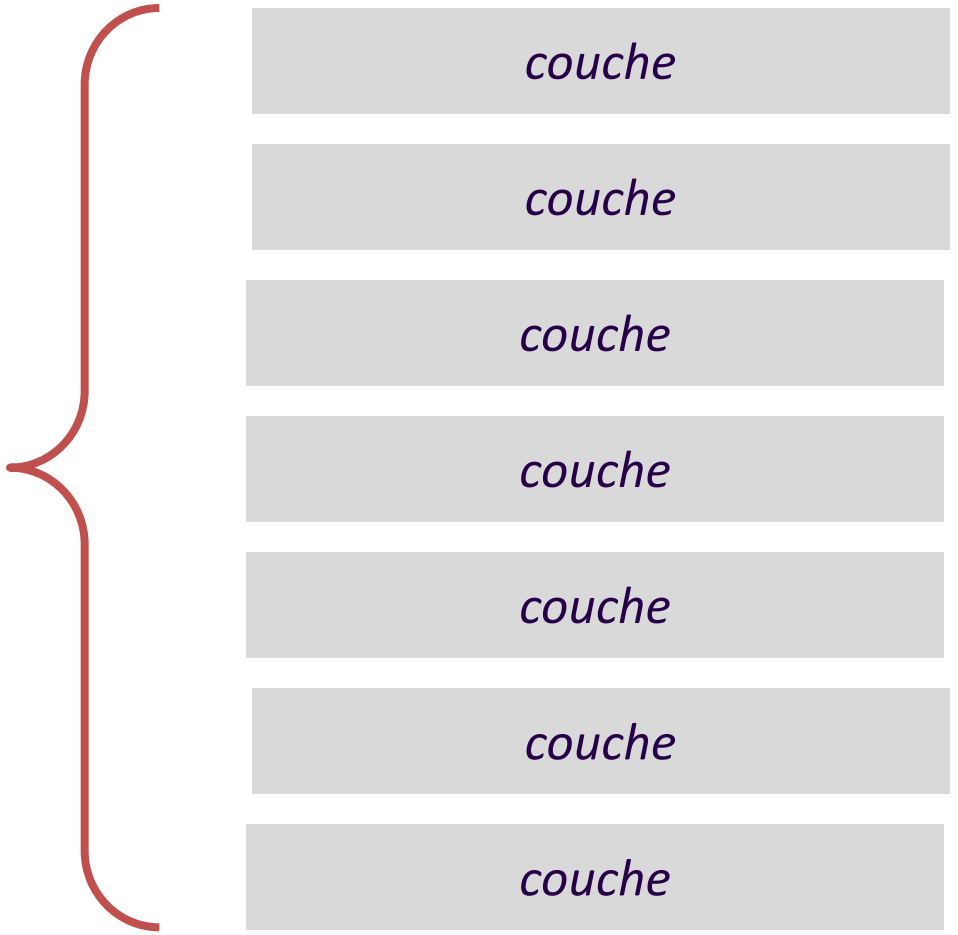
- Pourquoi un modèle pour les réseaux informatiques?
- Comprendre, concevoir et construire un réseau est une tache compliquée
- solution: subdiviser la tache en sous taches ou **couches (layers)**
- une couche est un ensemble homogène destiné à remplir une tache ou à rendre un service

Communication

Dans un réseau

informatique

Trés difficile

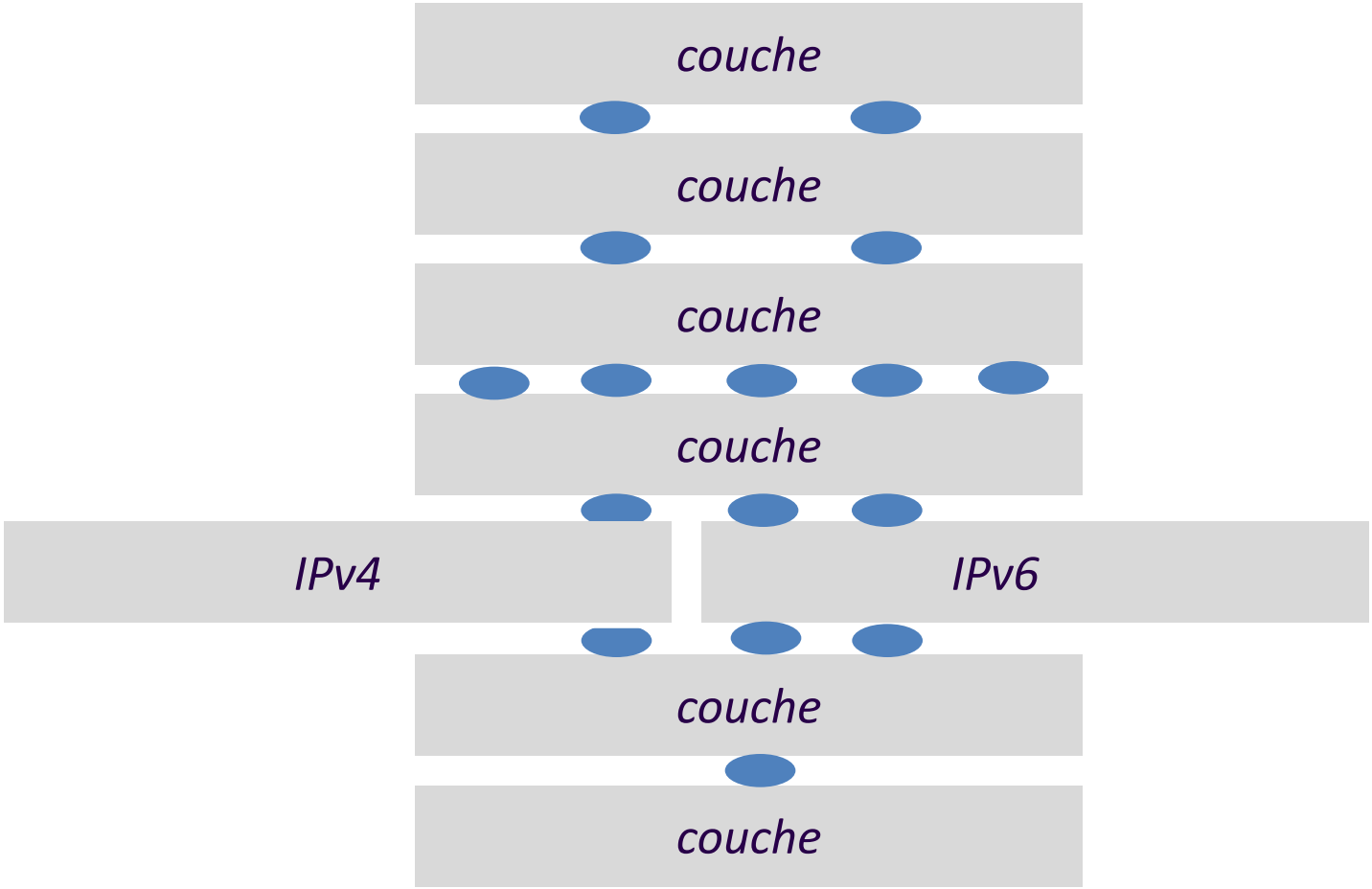


Modèle en couche

- Chaque couche exécute une ou plusieurs taches déterminées
- Chaque couche fournira un service à la couche supérieur et reçoit le service de la couche inférieur
- Changer une couche n'implique pas le changement de tout le système (changement de carte réseau ou de câble)

Communication verticale

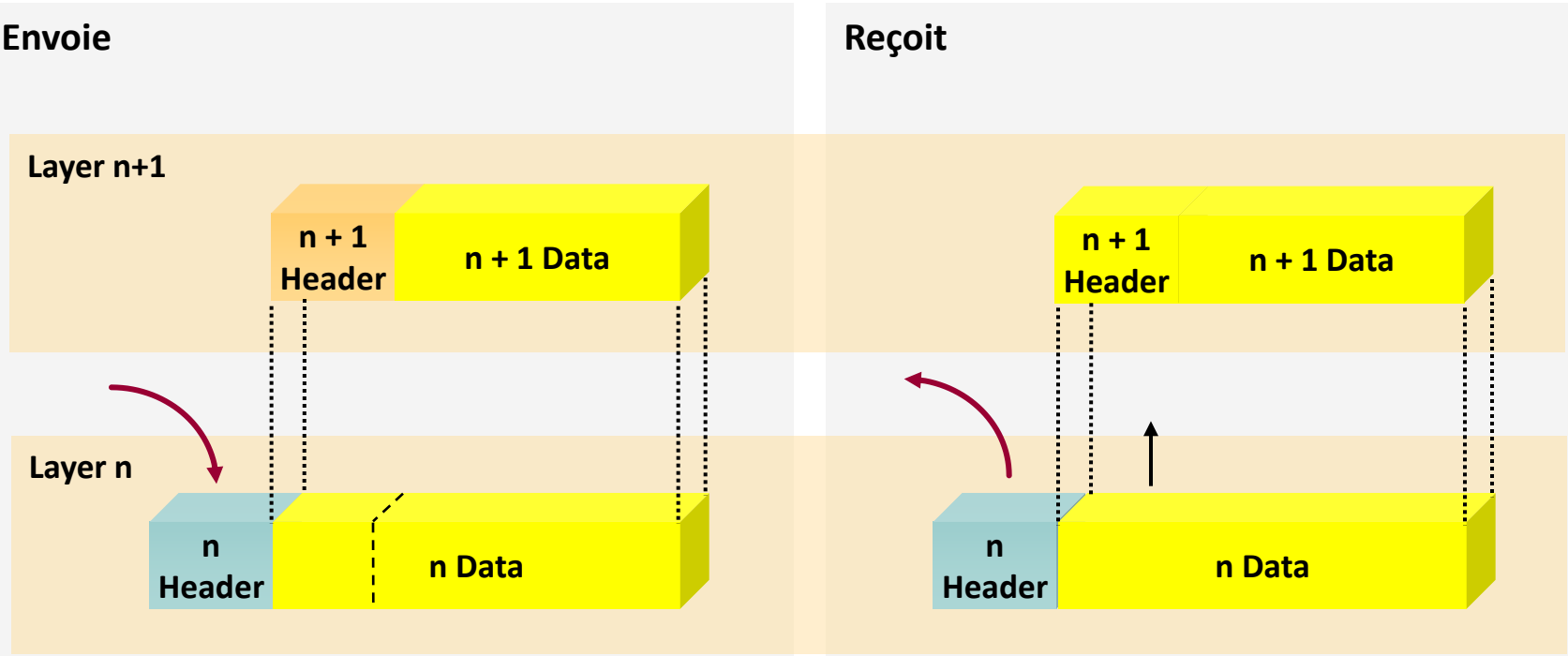
- La communication entre la couche n et n+1 se fait à travers un point d'accès appelé **Service Access Point SAP**
- Exemple: le numéro de port est le SAP vers l'application
- Il peut y avoir plusieurs SAP entre les couches
- la donnée passé par la couche supérieur à la couche inférieur est appelé **Service Data Unit SDU**


couche
couche
couche
couche
IPv4
IPv6
couche
couche

Encapsulation

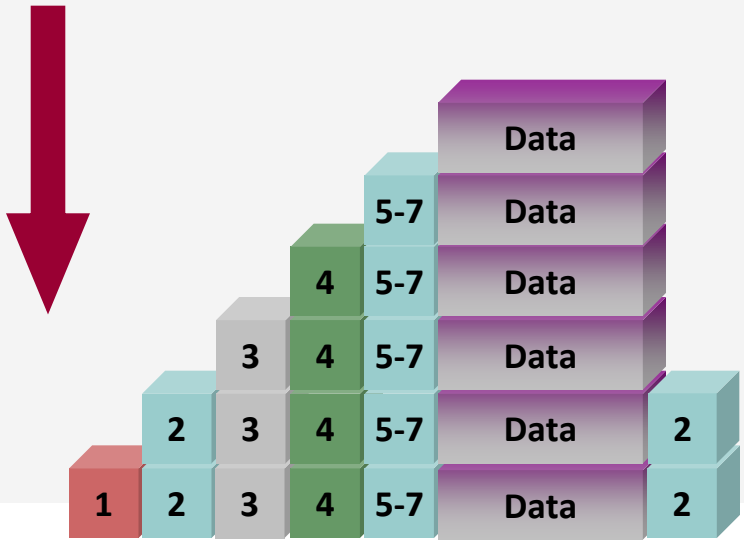
- La couche n envoie les données à la couche n-1 avec des informations spécifiques à la couche n sous forme d'**entête (header)**
- Les données transférées d'un noeud transitent par les couche du haut au bas en les **encapsulant** par des entête au fur et a mesure
- À la réception les données sont envoyées du bas vers le haut en **décapsulant** les entêtes

Transfert de données à travers les couches

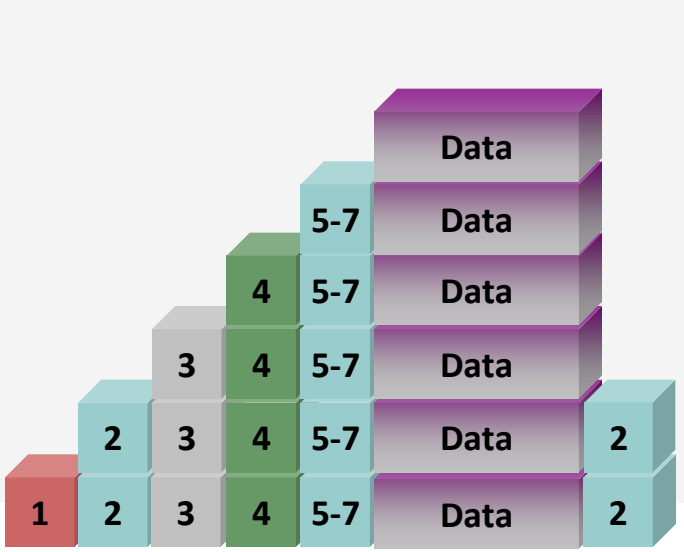


Envoie et reception de données dans le model en couche

Envoie

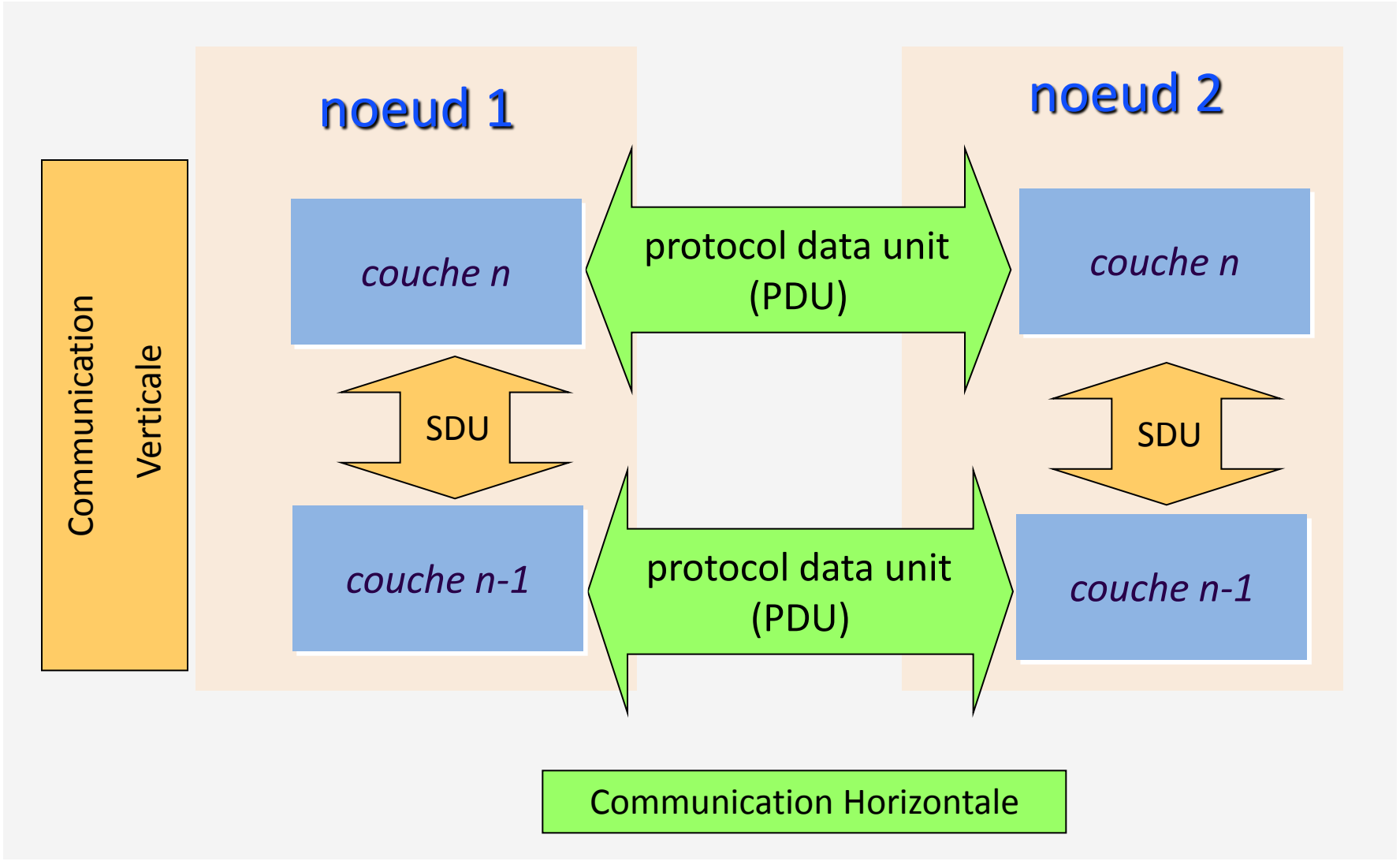


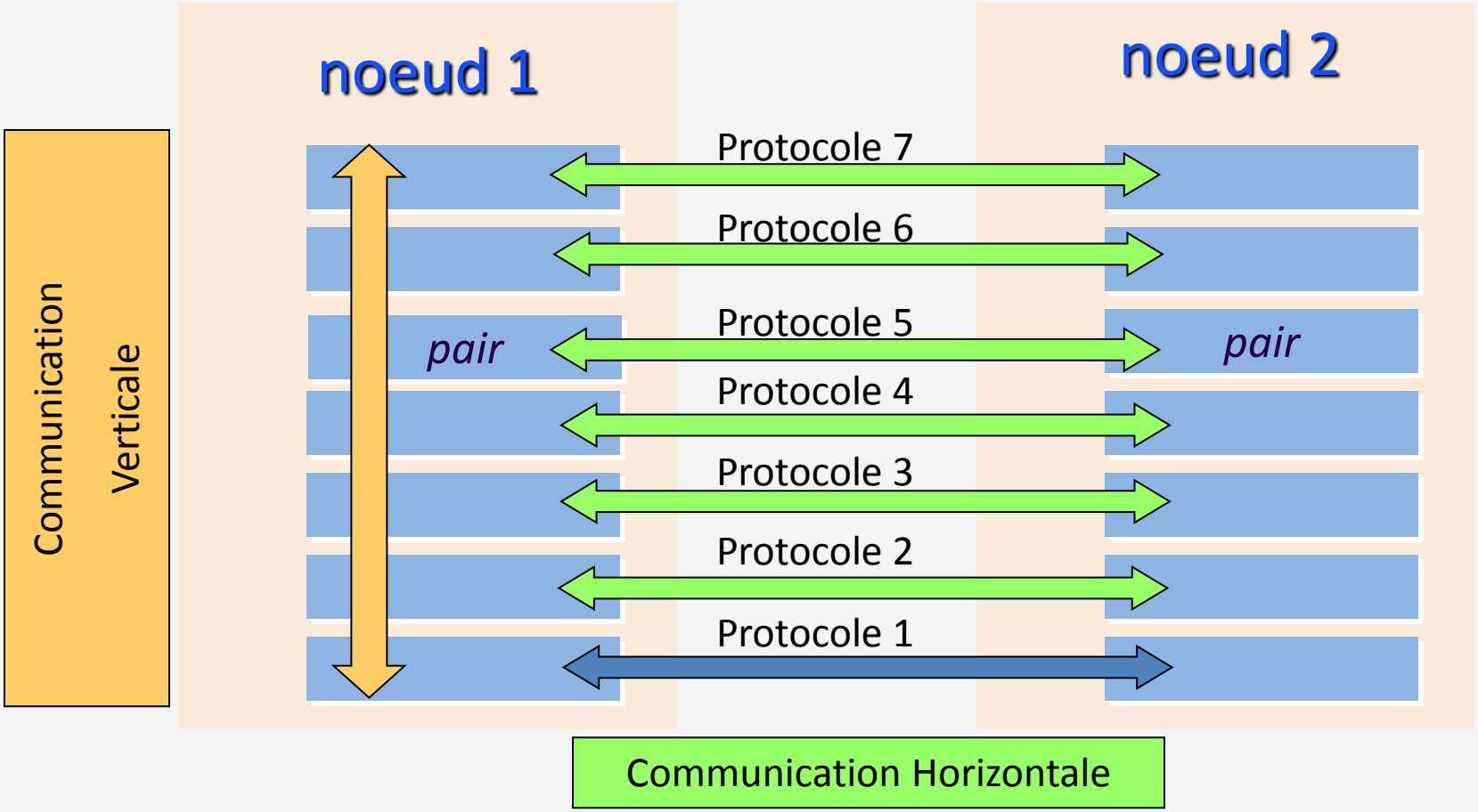
Reception



Communication entre couches

- Communication horizontale:
  - Chaque couche communique avec la couche du même niveau du pair correspondant selon **un protocole**
  - Cette communication est faite à travers la connexion verticale ou directement dans le cas de la couche la plus basse
  - Les données échangées sont appelées **Protocol Data Unit PDU**

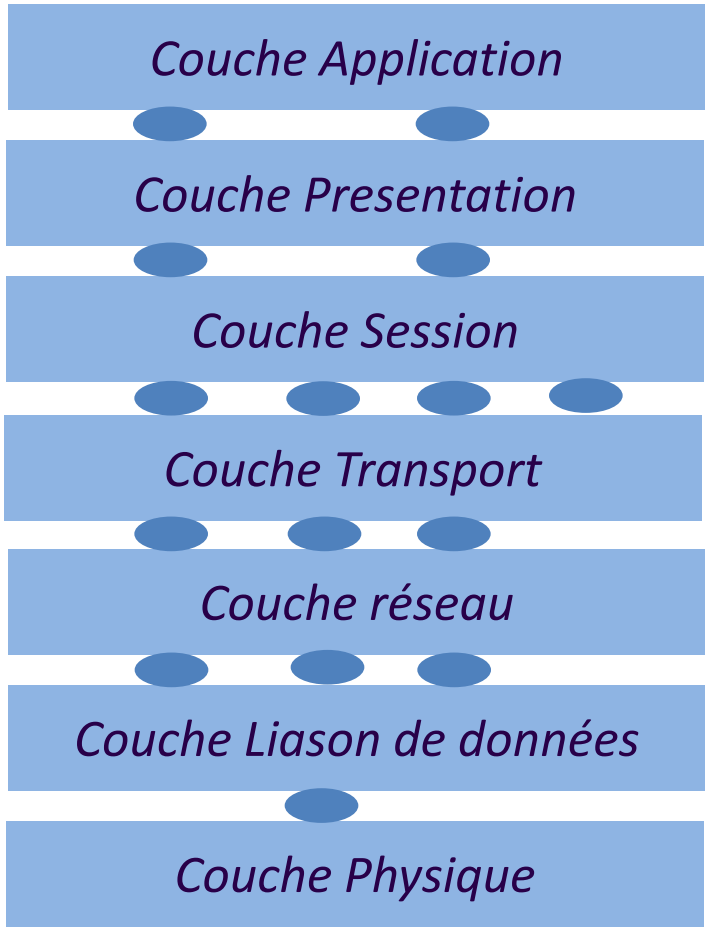

noeud 1
noeud 2
Communication Verticale
couche n
protocol data unit (PDU)
couche n
SDU
SDU
couche n-1
protocol data unit (PDU)
couche n-1
Communication Horizontale


noeud 1
noeud 2
Communication Verticale
Protocole 7
Protocole 6
Protocole 5
Protocole 4
Protocole 3
Protocole 2
Protocole 1
pair
pair
Communication Horizontale

Le modèle de référence OSI

- Historiquement chaque constructeur avait défini son modèle => architectures propriétaires donc non interopérable
- Nécessité de normalisation pour garantir l'interopérabilité
- OSI (Open System Interconnection) de l'ISO (international organization for standardization)
- Modèle en 7 couches
- les couches ont été définie avant les protocoles
- Une couche peut être divisé en sous couches

Le modèle de référence OSI



Couche Physique

- Transmet les bits de données sur un support physique
- Conversion des bits en signal électrique, électromagnétique ou optique
- Synchronisation entre transmetteur récepteur
- Types de connecteurs, de câbles
- Un nœud peut avoir plusieurs types de couches physique (carte réseau)

Couche Liaison de données

- Contrôle la transmission des trames à travers le lien
- Correction des erreurs dans les bits de données (checksum)
- Accorde l'accès au support dans le cas d'un média partagé
- Adressage physique dans le cas d'un média partagé
- Un noeud peut avoir plusieurs types de couches liaison de données selon les couches physiques existantes

Couche Réseau

- Trouver un chemin dans une série de lien et de nœuds
- Les nœuds dans le chemin doivent transférer (forward) le paquet dans la bonne direction
- Contrôle de congestion
- Fragmentation et réassemblage
- Adressage logique

Couche Transport

- Établissement d'une connexion de bout en bout (fiable ou pas)
- Correction d'erreur (perte de paquet au niveau réseau, duplication ou désordre)
- Fragmentation et réassemblage (éviter la fragmentation au niveau réseau)
- Contrôle de flux
- Multiplexage

Couche Session

- Contrôle de dialogue entre les terminaux communicants(initiation, arrêt et redémarrage)
- Enchaînement et cohérence (un groupe de paquets n’est pas délivré si un paquet est absent)

Couche Présentation

- Représentation des données pour l'application
- La couche présentation remplit trois fonctions principales:
  - codage et conversion des données de la couche application afin que les données issues du périphérique source puissent être interprétées par l'application appropriée
  - compression des données de sorte que celles-ci puissent être décompressées par le périphérique de destination
  - chiffrement des données à la transmission et déchiffrement des données à la réception

Couche Application

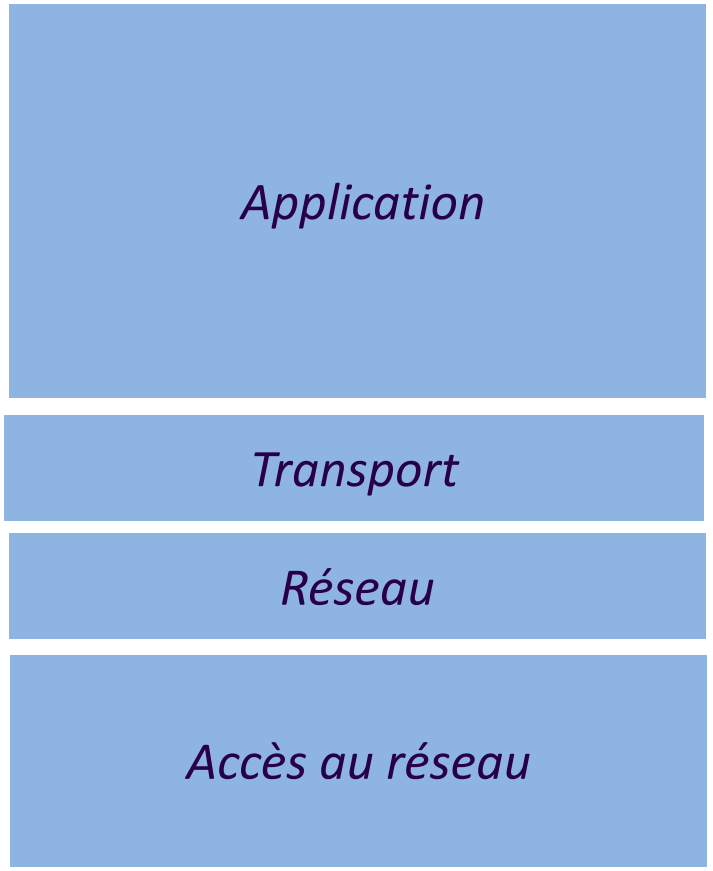
- Transfert de fichier, le web, vidéoconférence
- PS: les trois dernières couches sont en général incluses dans la couche application

PDU par couche

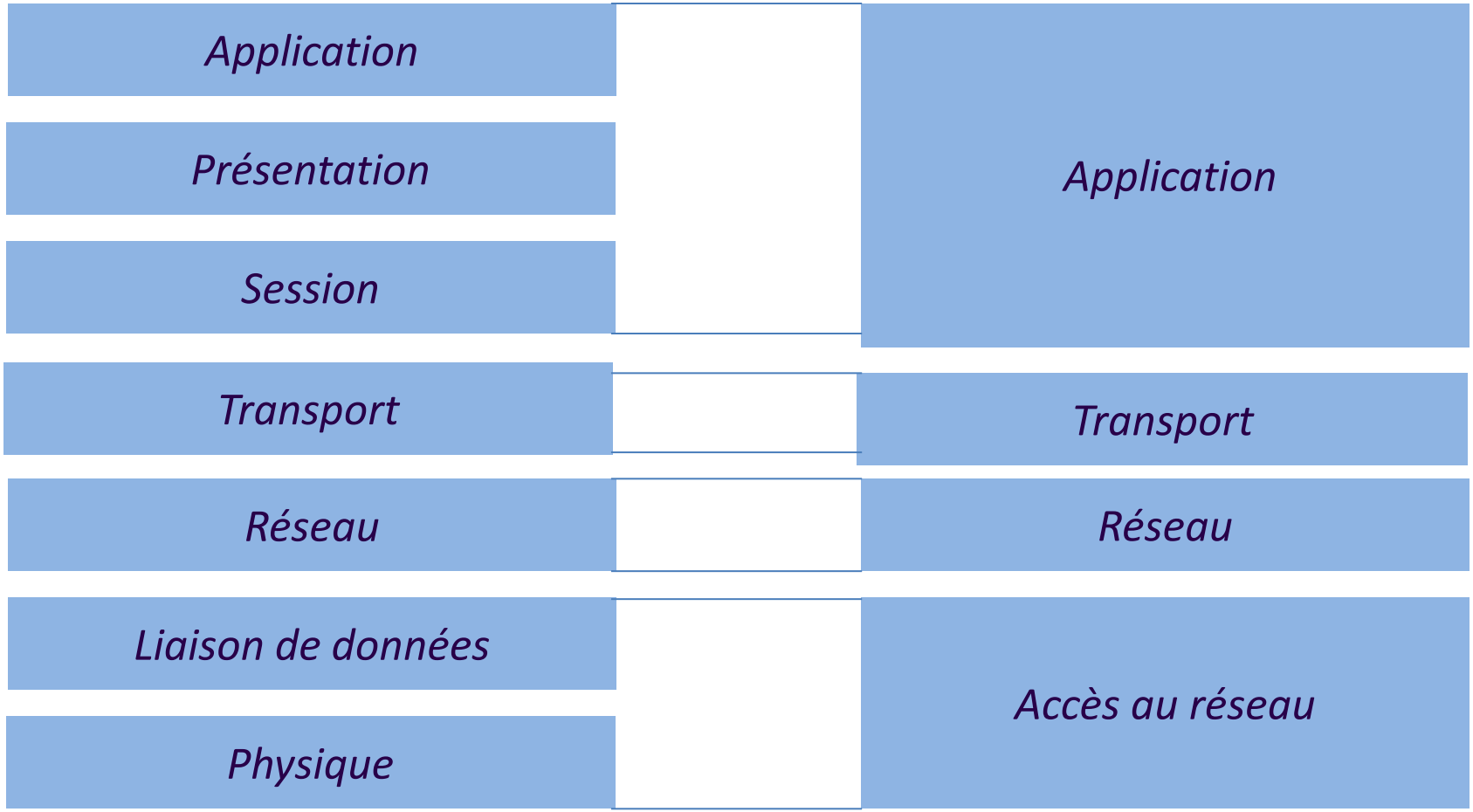
- Donnée => application
- Segment => transport
- Paquet => réseau
- Trame => liaison de données
- Bit => physique

Modèle TCP/IP

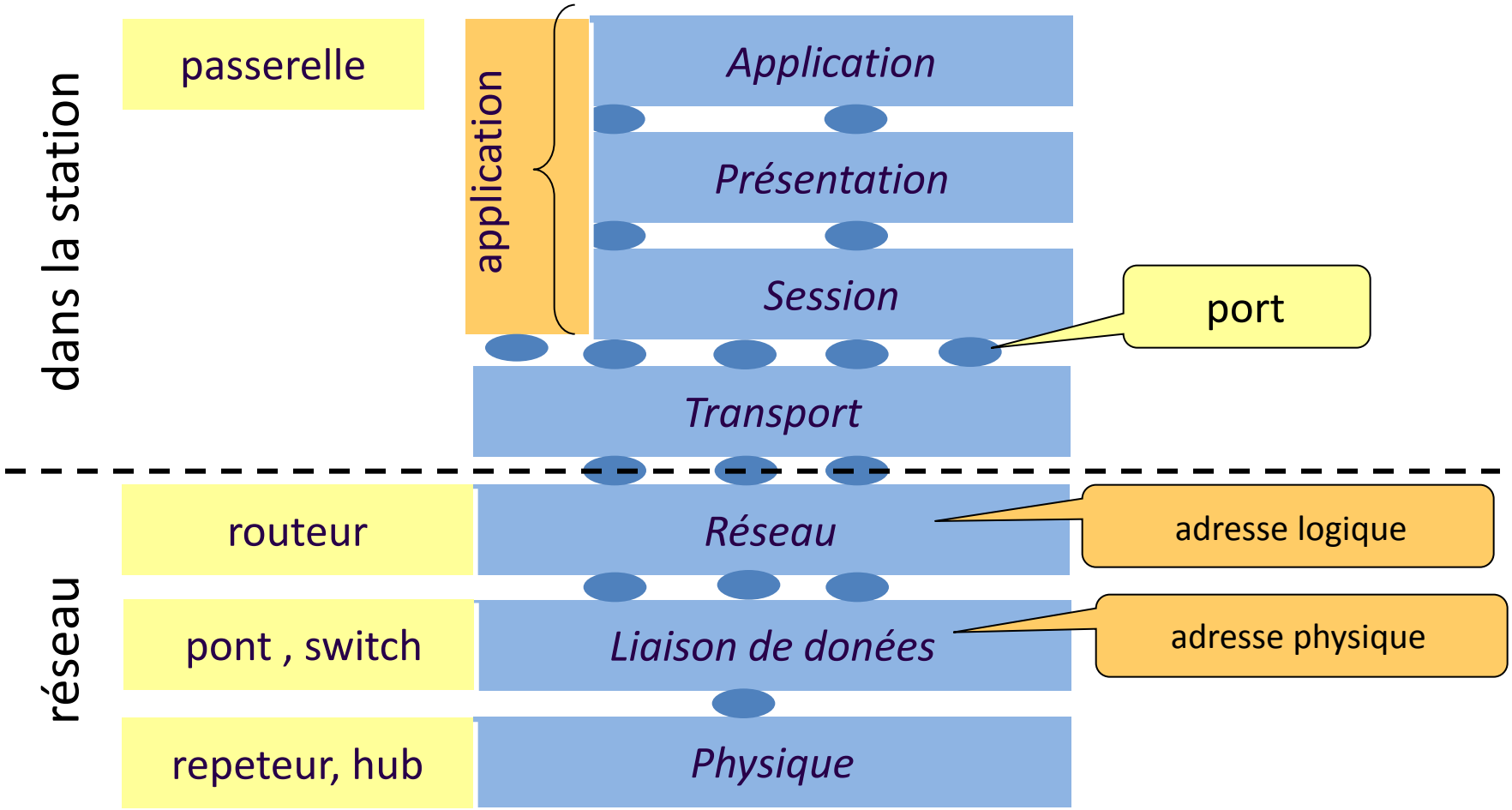
- C’est le modèle le plus utilisé
- Il a précédé le modèle OSI
- TCP/IP est une norme ouverte ne respectant pas le modèle OSI
- l’IETF est l’organisation responsable des normes de l’internet
- Les documents qui décrivent ces normes (protocoles) s’appellent des RFC (Request for Comment)



OSI versus TCP/IP



Périphériques réseau



La couche physique

objectif

- La couche physique fournit le moyen de transporter sur le support réseau les bits constituant une trame de la couche liaison de données
- La transmission de trames sur le support local exige les éléments de couche physique suivants :
  - Le support physique et les connecteurs associés
  - Une représentation des bits sur le support
  - L'ensemble de circuits émetteur et récepteur sur les périphériques réseau

Rôle de la couche physique

- Le support ne transporte pas la trame comme entité unique. Il transporte les signaux qui représentent les bits individuellement
- Il existe trois formes élémentaires de support réseau :
  - Câble de cuivre => signal électrique
  - Fibre => signal lumineux
  - Sans fil => onde électromagnétique

normalisation

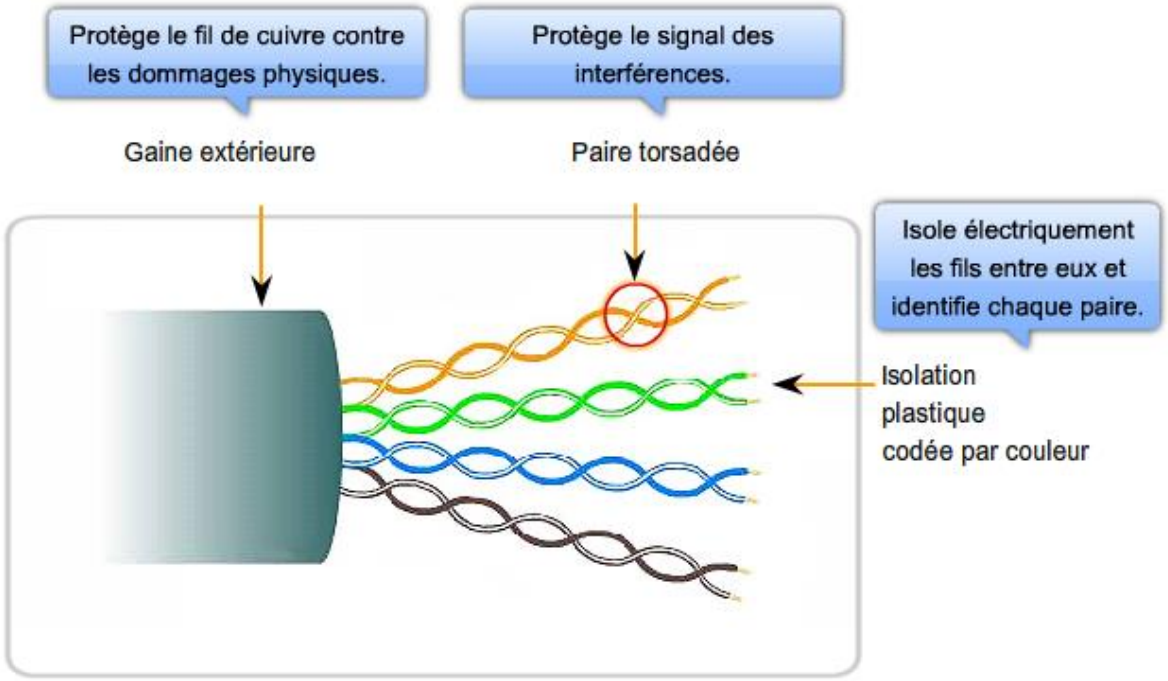
- les propriétés physiques, électriques et mécaniques des supports sont définis par des organisme de normalisation=> garantir l'interopérabilité
- Les propriété pour un support de cuivre:
  - Le type de câblage en cuivre utilisé (paires torsadées, cable coaxial…)
  - La bande passante de la communication
  - Le type de connecteurs utilisés
  - Le brochage et les codes couleur des connexions avec le support
  - La distance maximale du support

exemple

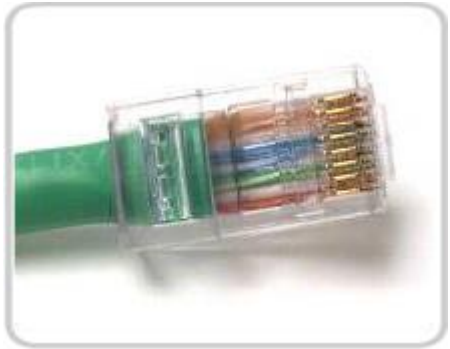
- EIA/TIA: (Electronics Industry Alliance/Telecommunications Industry Association)

	10BASE-T	100BASE-TX	100BASE-FX	1000BASE-CX	1000BASE-T	1000BASE-SX
Supports	EIA/TIA catégorie 3, 4, 5 UTP, quatre paires	EIA/TIA catégorie 5 UTP, deux paires	Fibre multimode de 50/62.5 microns	STP	EIA/TIA catégorie 5 (ou supérieure) UTP, quatre paires	Fibre multimode de 50/62.5 microns
Longueur maximale des segments	100 m	100 m	2 km	25 m	100 m	Jusqu'à 550 m selon la fibre utilisée
Topologie	En étoile	En étoile	En étoile	En étoile	En étoile	En étoile
Connecteur	ISO 8877 (RJ-45)	ISO 8877 (RJ-45)		ISO 8877 (RJ-45)		

Câble UTP

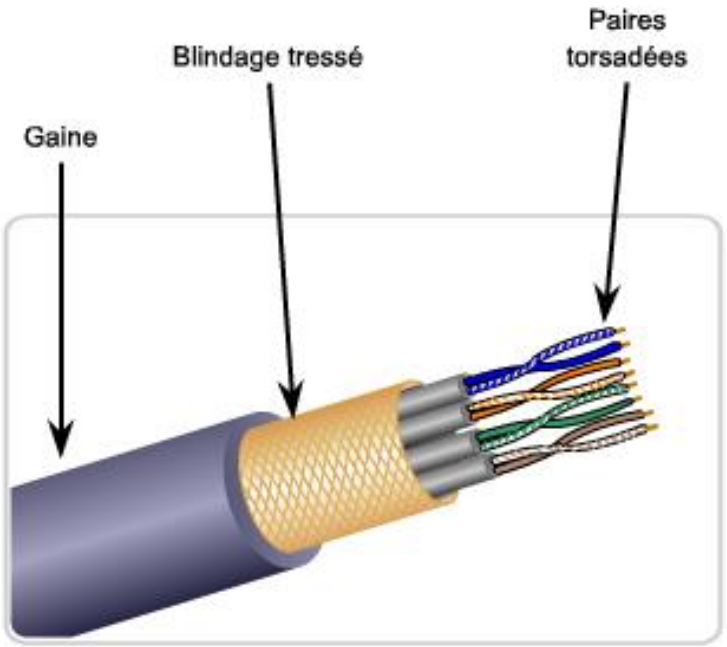


Connecteur RJ45:



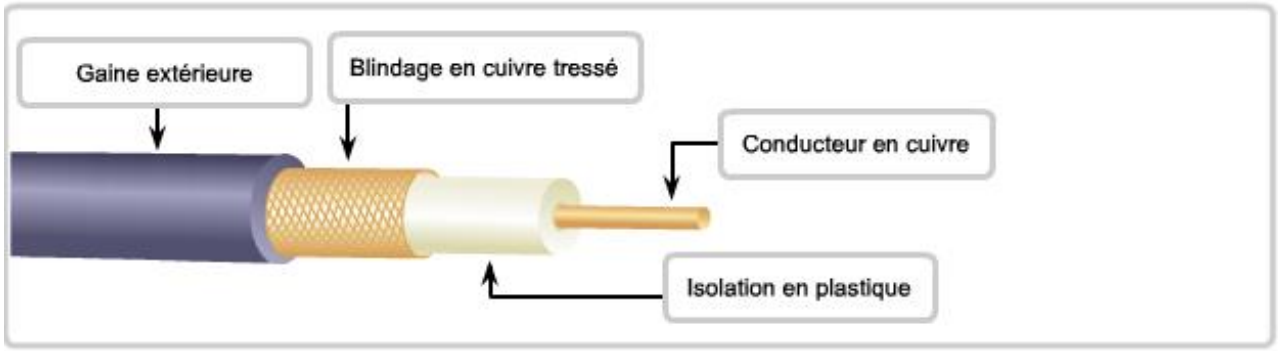
Câble STP

- Shielded twisted Pair: paires torsadées blindées
- Plus chère que le câble UTP et de moins en moins utilisé



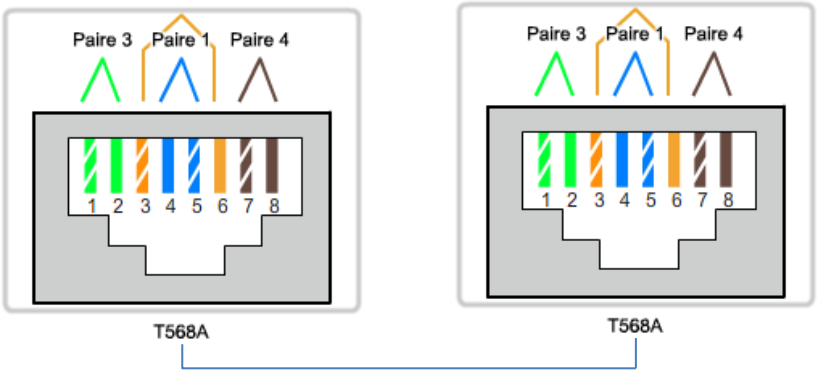
Câble coaxial

- Très utilisé dans la diffusion télé
- Était utilisé par les premières normes de Ethernet (10base2)

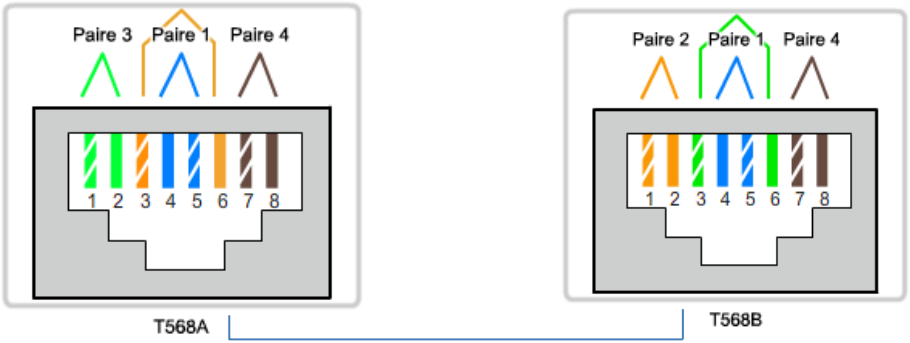


Câble droit/croisé

- Ethernet droit: les deux extrémité T568A ou T 568B



- Ethernet croisé: une extrémité T568A et l'autre T568B



Utilisation des câbles droits/croisés

- Une pair de transmission Tx (1 et 2) et une pair de réception Rx (3 et 6)
- Le croisement se fait avec un équipement d'interconnexion de type Hub ou switch
- Câble droit: connecter une machine à un hub ou à un switch
- Câble croisé: connecter une machine à une autre machine ou une machine à un routeur
- De nouvelles cartes réseaux peuvent détecter automatiquement l'état du câble (droit ou croisé) et faire un croisement à la source (auto MDI-MDIX)=> machine à machine avec un câble croisé

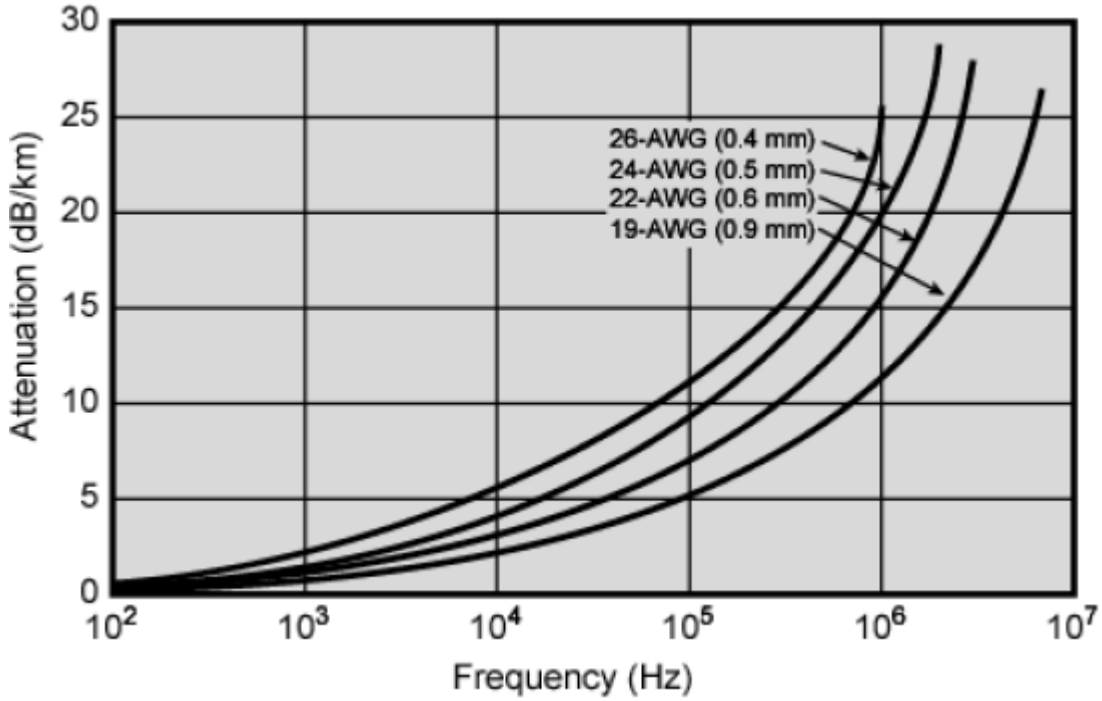
Critères de choix de câble

- Prix de fabrication: les fibres optiques > câbles coaxiaux > paires torsadées
- Résistance aux perturbations:
  - Les parasites: perturbations venues de l'extérieur du câble ou bruit => ex: champ magnétique émanant d'un câble d'électricité
  - L'affaiblissement: c'est une perte d'énergie le long du câble=> le signal de sortie est plus faible que le signal d'entrée

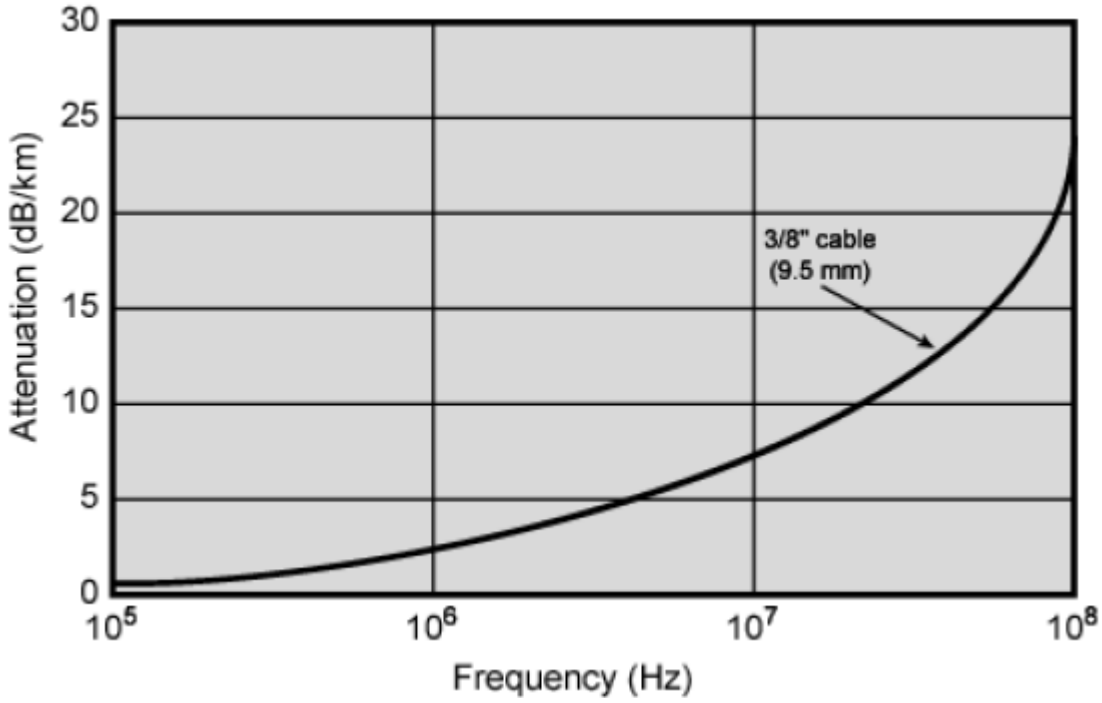
Affaiblissement du signal

- L'affaiblissement dépend de
  - La longueur du câble : plus le câble est long plus l'affaiblissement est important
  - Le type du support: plus le câble est mince plus l'affaiblissement est important
  - La fréquence du signal transmis: plus la fréquence est élevé plus l'affaiblissement est important

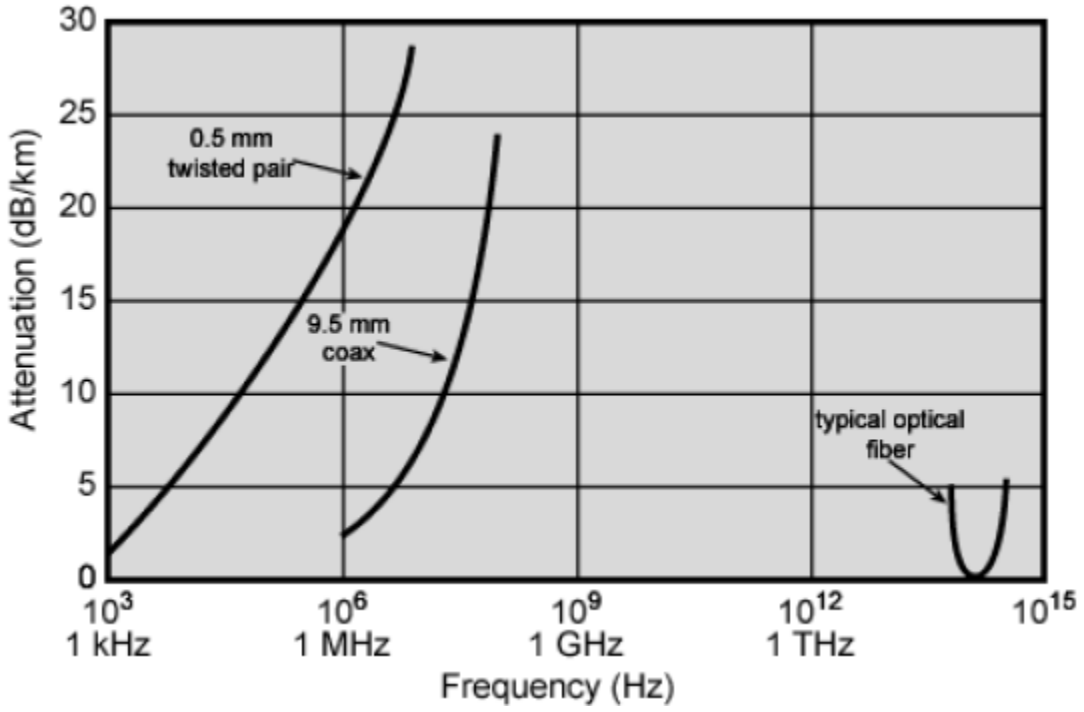
Paires torsadées



Câble coaxial



comparaison



Transmission en bande de base

- Un signal est transmis en bande de base lorsqu'il ne subit pas une transposition de fréquence
- La bande de fréquence va de la proximité de 0 à une fréquence de coupure
- Utilisée dans la transmission en réseau locaux => courte distance
- La transmission en bande de base utilise toute la bande passante du support => impossibilité de multiplexage

Codage de l’information

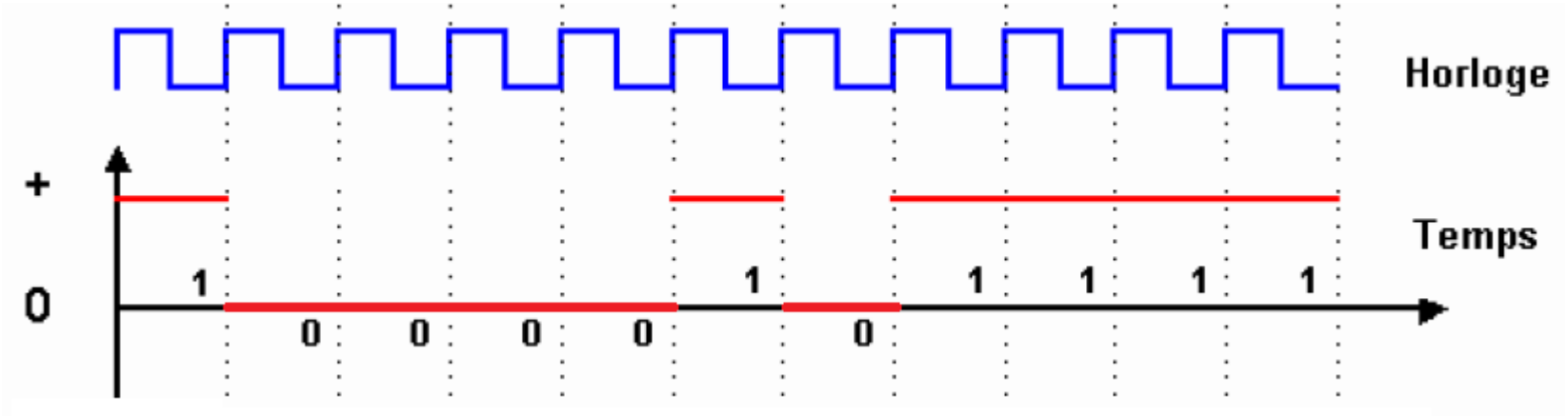
- Comment transmettre le 0 et 1 sur le support physique?
- On doit coder cette information sous forme d’un signal ayant au moins deux états=> appelé aussi codage en ligne
- Les états peuvent être deux niveaux de tensions ou d’intensité lumineuse par exemple

Codage de l’information

- Le type de codage doit optimiser l’utilisation du support:
  - Minimisation de l’atténuation
  - Maximisation du débit
  - Maintenir la synchronisation dans le cas des réseaux asynchrone (l’horloge n’est pas transmise) c’est le cas d’Ethernet par exemple

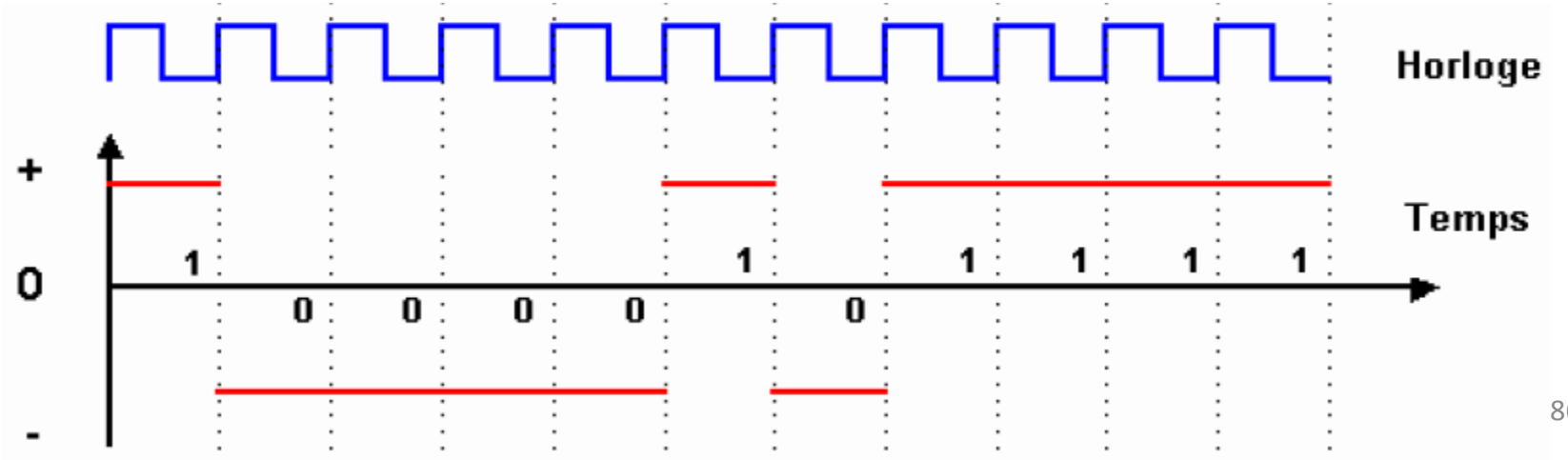
Codage RZ

- RZ: Return to Zero (retour à Zéro)
- Codage binaire: 1 correspond à l'existence de tension et 0 à l'absence de tension
- Inconvénient: le niveau 0V correspond aussi à un câble défaillant, problème de synchronisation



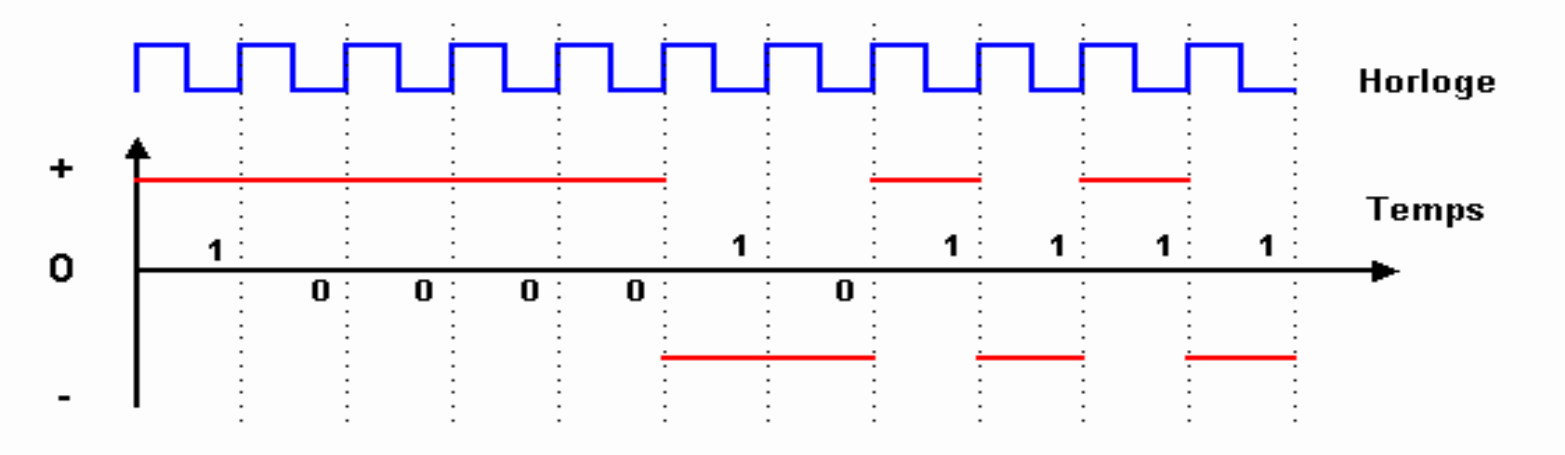
Codage NRZ

- NRZ: No Return to Zero (non retour à zero)
- 1 correspond à +V et 0 à –V
- NRZ améliore le codage RZ en augmentant la différence d'amplitude (minimiser l'atténuation)
- Inconvénient: de longues bit à 1 ou 0 engendrent une perte de synchronisation



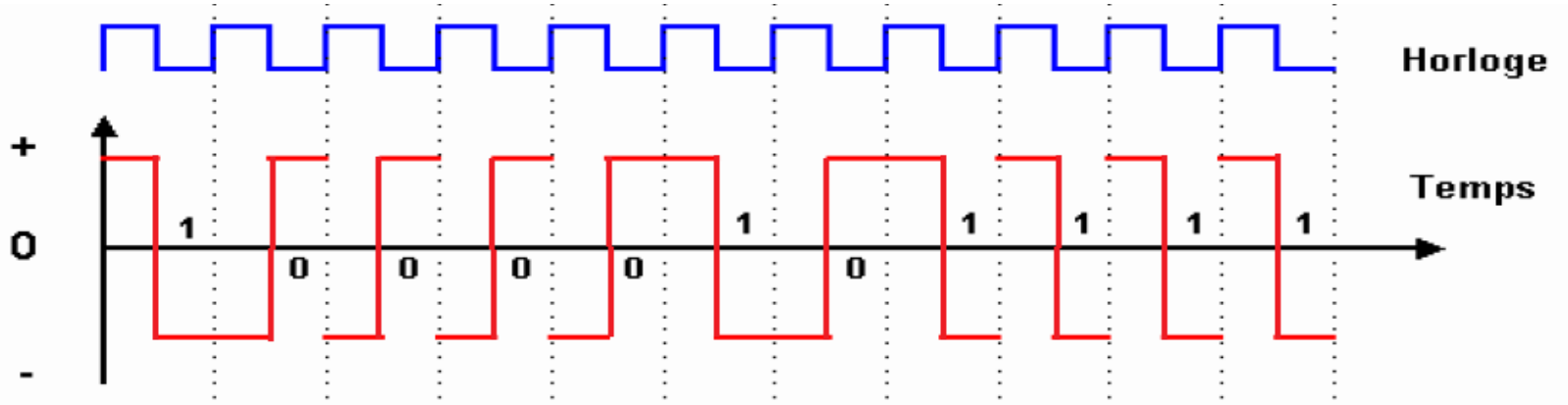
Codage NRZI

- No Return to Zero Inverted
- Principe: on produit une transition pour 1, pas de transition pour 0
- Inconvénient: une longue série de 0 provoque une longue période sans transition => perte de synchronisation



Codage Manchester

- Déclencher une transition à chaque bit envoyé
- 1 est représenté par la transition +V à –V et 0 est représenté par la transition –V à +V
- La synchronisation est assurée même avec de longues série de 0 ou de 1, ce codage est peu sensible aux erreurs
- Le codage Manchester est utilisé par Ethernet 10Mbit/s (10baseT)
- Inconvénient: Les transitions augmentent la fréquence du signal=> débit limité



Comment augmenter le débit?

- Pour augmenter le débit il faut limiter la fréquence du signal tout en ayant suffisamment de transitions
- Solution : il faut utiliser deux codage simultanément

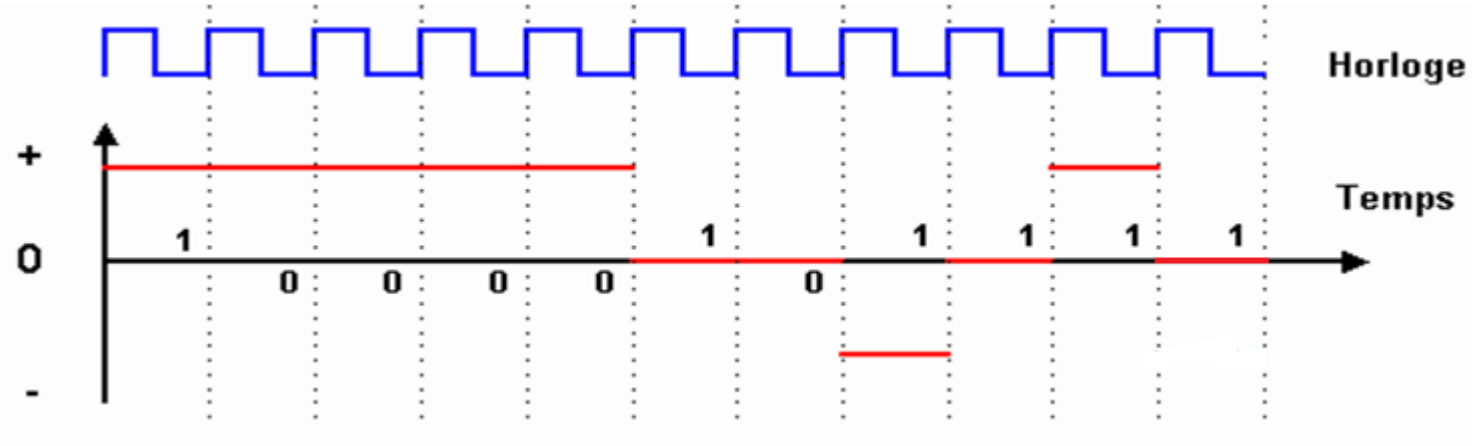
Codage 4B/5B

- Principe: on code un groupe de 4 bit en 5bits en utilisant une table de transcodage
- Le message à transmettre contiendra au plus trois 0 consécutifs => plus de transitions (augmentation de la fréquence)
- Plusieurs mot en 5 bits ne sont pas utilisés: ils sont utilisés pour le contrôle de transmission ou début/fin d'une trame

Groupe de 4 bits	Symbole 4B5B
0000	11110
0001	01001
0010	10100
0011	10101
0100	01010
0101	01011
0110	01110
0111	01111
1000	10010
1001	10011
1010	10110
1011	10111
1100	11010
1101	11011
1110	11100
1111	11101

Codage MLT3

- Multi level transmit 3 (3niveaux)
- Principe: seuls les 1 font changer l'état du signal, les 0 conserve le même état
- Les 0 et 1 sont codés sur trois états +V, 0 et –V
- Ce codage diminue fortement la fréquence du signal
- Les réseaux fast Ethernet (100baseTX) utilisent le codage 4B/5B associé au codage MLT3



exercice

- Coder la chaine de bits suivante avec les différents codes 01110000000101010011
- Comparer les résultats
- Quel inconvénient présente l'utilisation du code 4B5B?

Limitation de la transmission en bande de base

- Il existe une relation entre le nombre maximal de symboles par seconde que le support peut admettre et la bande passante
- **Critère de nyquist**: $R \leq 2*BP$ ou R est la rapidité de modulation en bauds (nombre de symboles par seconde) et BP est la bande passante en Hz
- **Le débit binaire**: $D=R*\log_2 v$ ou v est la valence qui est le nombre d'état que peut prendre un symbole (exemple la valence du codage NRZ est 2)

Limitation de la transmission en bande de base

- Pour augmenter de débit binaire il faut augmenter la bande passante ou la valence
  - La BP est limité par la nature du support physique
  - La valence est limitée par le bruit
- Le bruit rend les niveaux d'amplitude difficile à être distingués par le système de réception
- **Relation de shannon** $vmax = \sqrt{1 + \frac{S}{N}}$
  - Capacité maximale de transmission d'un canal $C=BP*\log_2(1+S/N)$

Transmission en large bande

- La transmission en bande de base limite la longueur du réseau
- Pour envoyer un signal sur une distance plus longue il faut le moduler
- Utilisation d'un modem (modulateur/démodulateur)

ETTD/ETCD

- Un équipement de traitement de données ETTD ou DTE en anglais (data terminal equipement) est un élément susceptible d'échanger des données avec un réseau, qui ne se connecte pas directement à la ligne de transmission. Par exemple : un ordinateur, un terminal, une imprimante
- La connexion à la ligne de transmission se fait à travers un ETCD (équipement terminal de circuit de données) ou DCE en anglais (data circuit-terminating equipement), cet équipement adapte le signal aux conditions de la ligne, exemple: modem

Types de modulation

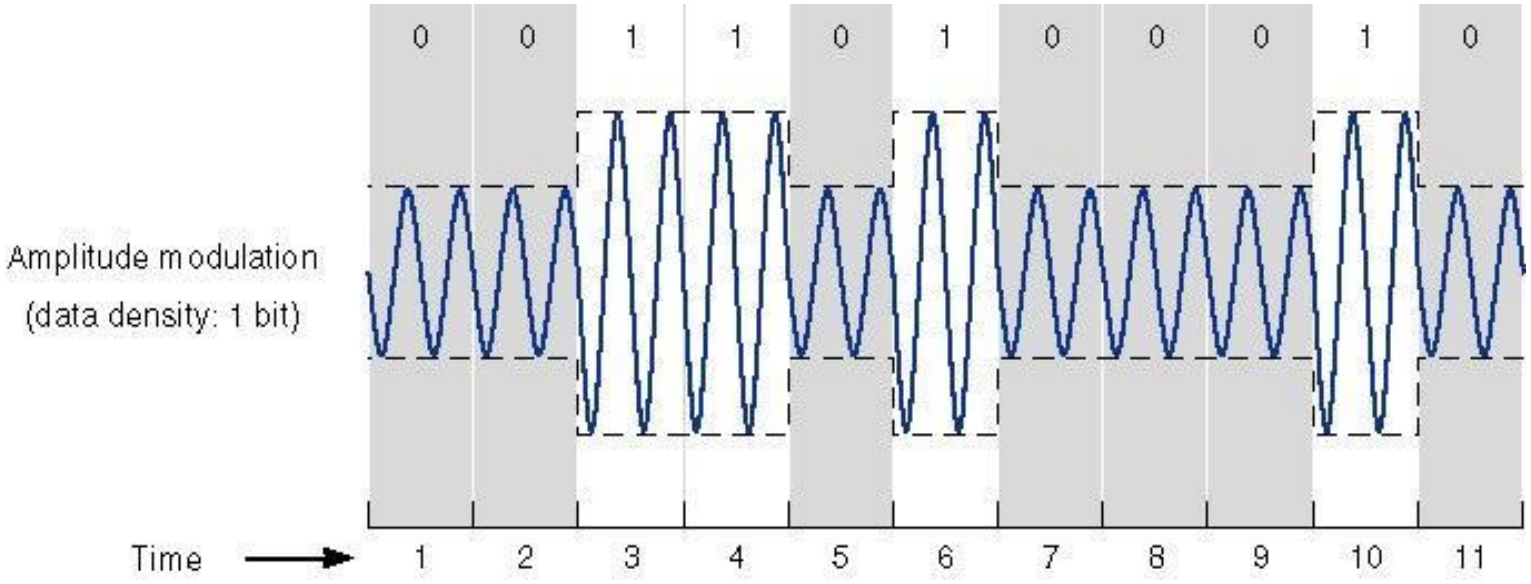
- On utilise une porteuse sinusoïdale

$$s(t) = A\sin(2\pi ft + \phi)$$

- les bits sont codés sur les paramètres caractéristiques de la porteuse:
  - amplitude A
  - fréquence f
  - la phase Φ

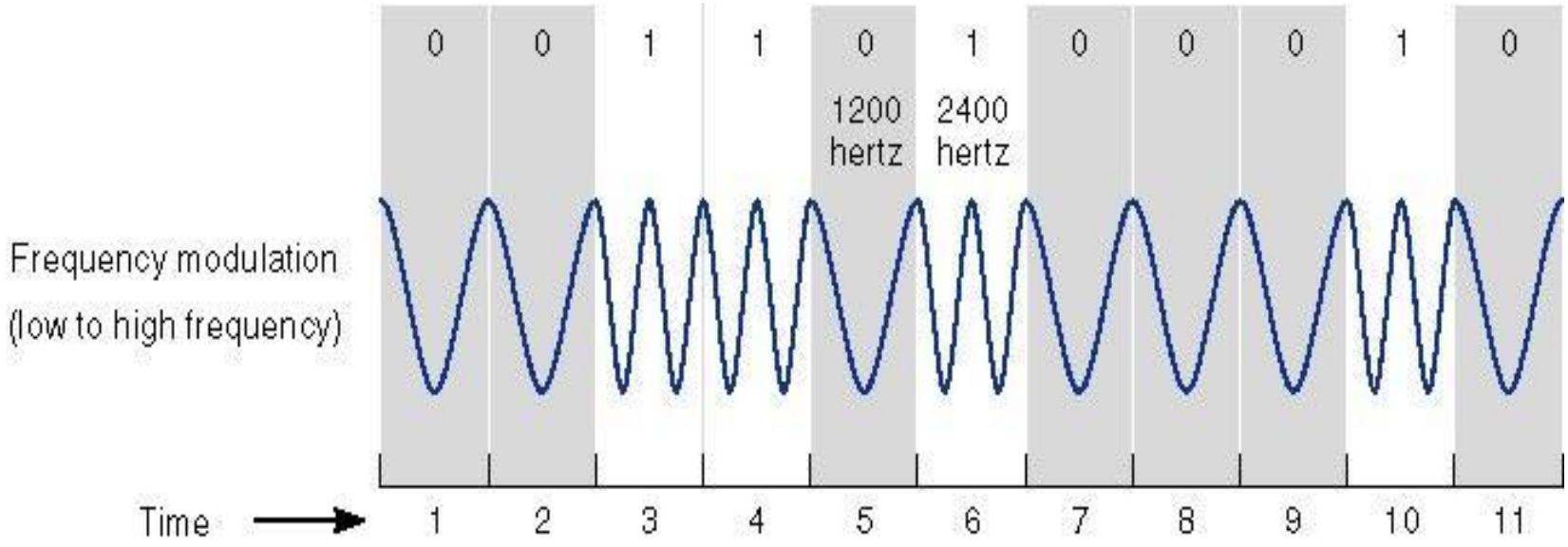
Modulation d'amplitude

- Les bits sont codés avec des amplitudes différentes



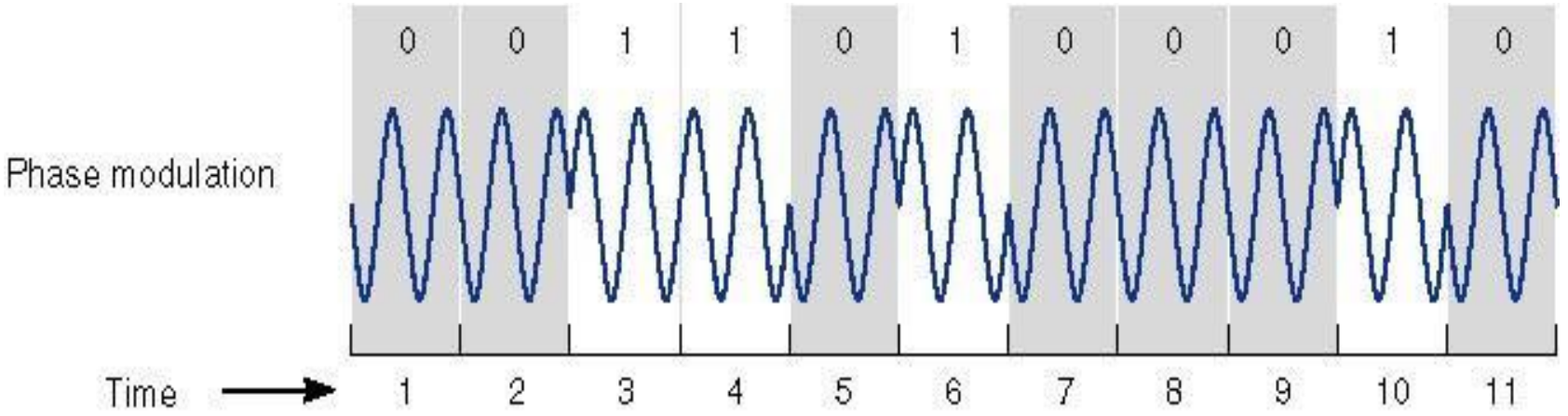
Modulation de fréquence

- Les bits sont codés avec des fréquences différentes



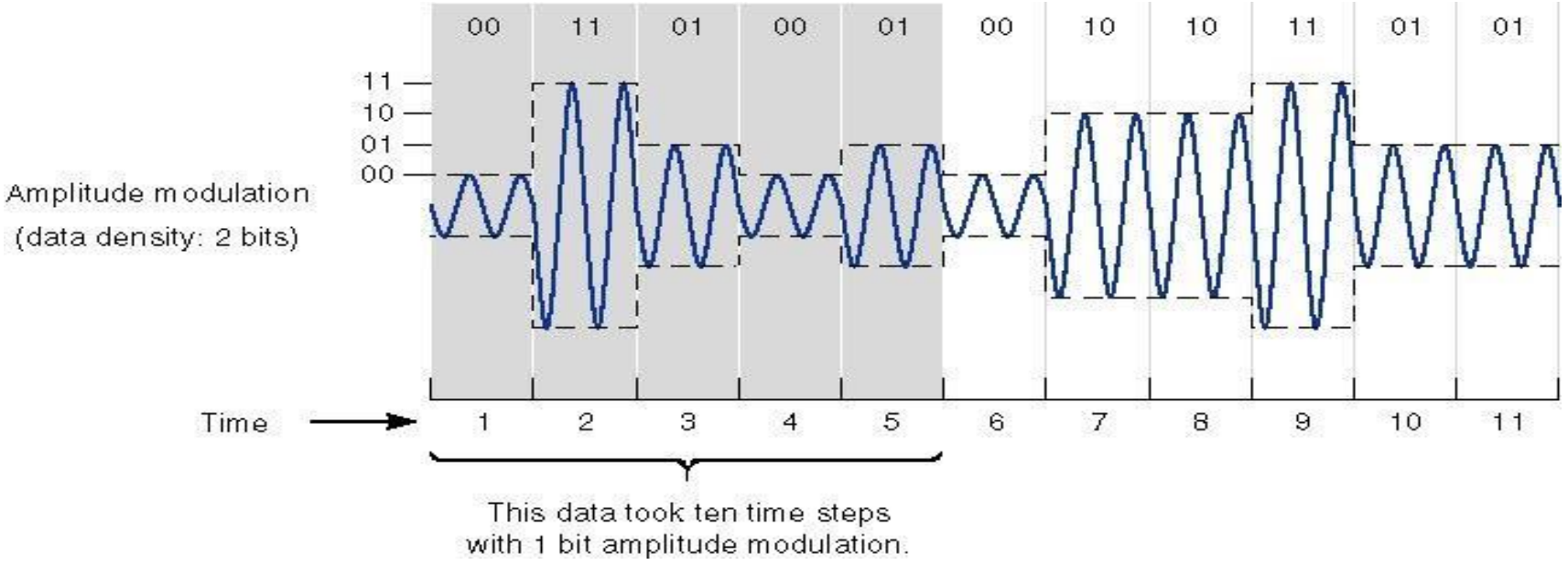
Modulation de phase

- Les bits sont codés avec des phases différentes



Modulation de plus d'un bit

- Différents niveaux d'amplitudes (de fréquences ou de phases) selon le nombre de combinaisons possibles
- Soit n le nombre de bit à moduler par un état le nombre d'états nécessaire est 2^n



Le multiplexage

- Le multiplexage permet de partager un support de communication entre plusieurs sources
- L'installation et l'entretien d'une seule liaison est beaucoup moins cher que plusieurs liaisons à bas débit
- Un multiplexeur mets deux ou plusieurs transmissions sur un seul support de communication
- généralement la capacité du support de multiplexage doit être égale à la somme des capacités des lignes multiplexées

Schéma générale

Multiplexage

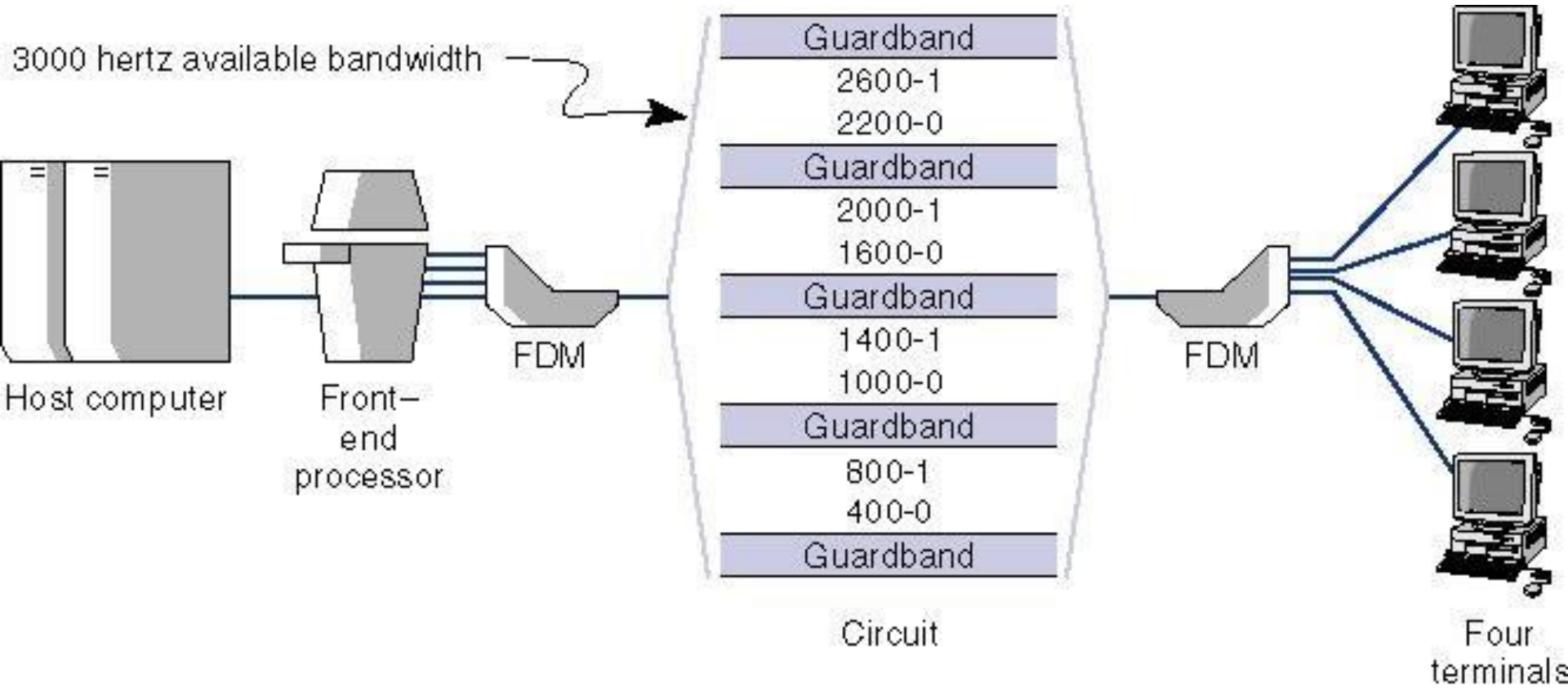
Il y a trois types majeurs de multiplexage

- Multiplexage fréquentiel ou Frequency division multiplexing (FDM)
  - Radio, Téléphonie analogique
- Multiplexage temporel ou Time division multiplexing (TDM)
  - Téléphonie numérique ou RNIS
- Multiplexage à longeur d'onde ou Wavelength division multiplexing (WDM)
  - Utilisée dans la transmission sur fibre optique

Frequency Division Multiplexing (FDM)

- Les multiplexeurs de fréquence divisent la bande en plusieurs canaux chaque communication occupe un canal.
- Bandes de garde sont utilisées pour protéger le canal contre les éclaboussures des autres canaux
- Les multiplexeurs de fréquence sont inflexible, une fois le nombre de canaux sont déterminés il est difficile d'ajouter de nouveaux canaux
- L'utilisation des bandes de garde constitue un gaspillage de ressources

Frequency Division Multiplexing (FDM)

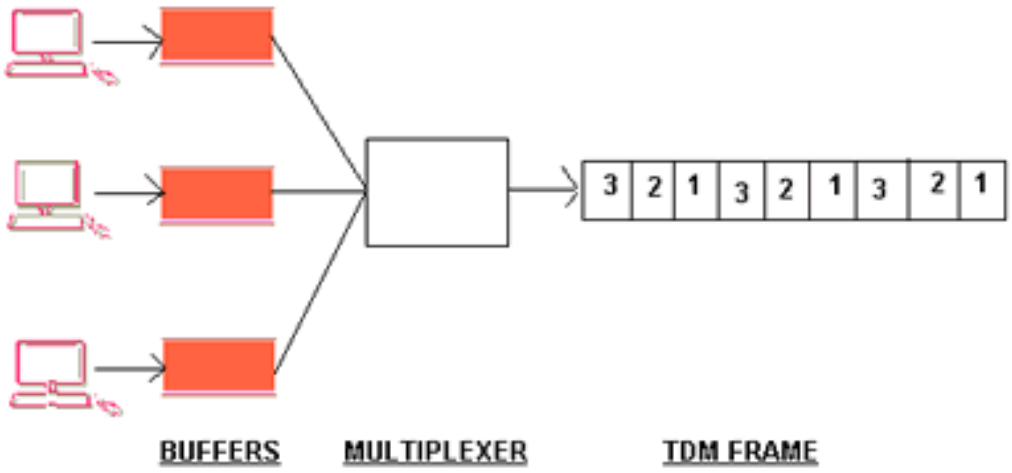


Time Division Multiplexing (TDM)

- Le multiplexage temporel divise le temps d'occupation de toute la bande de la liaison haut débit entre les communications à multiplexer
- Le temps est alloué sur la liaison haut débit pour chaque liaison bas débit
- Le multiplexage TDM est en général plus efficace que le multiplexage FDM est moins cher à implémenter et plus flexible

Multiplexage temporel synchrone

- Le démultiplexeur connait la provenance de chaque donnée à partir de sa position dans la trame
- Le débit sur les liaisons bas débit doit être constant
- Les slot sont allouée même en l'absence de données à transmettre=> gaspillage de ressources



Multiplexage temporel statistique

- Le multiplexage temporel statistique permet de multiplexer des liaisons avec des débits variables
- L'allocation des slots varie selon la quantité d'information transmise par chaque liaison bas débit
- La synchronisation est perdue (on ne sait plus l'ordre des données transmises)=> l'information sur la destination doit être incluse avec les données (partie signalisation)=> overhead = gaspillage de ressources

Support en fibre

- Câble de fibre en verre ou en plastique pour guider les imputions de la source à la destination
- Il dispose d'une bande passante très élevée
- La fibre n'est pas exposée à la perturbation des champs magnétique
- La déperdition du signal est très faible => longues distances

Mise en place de la fibre

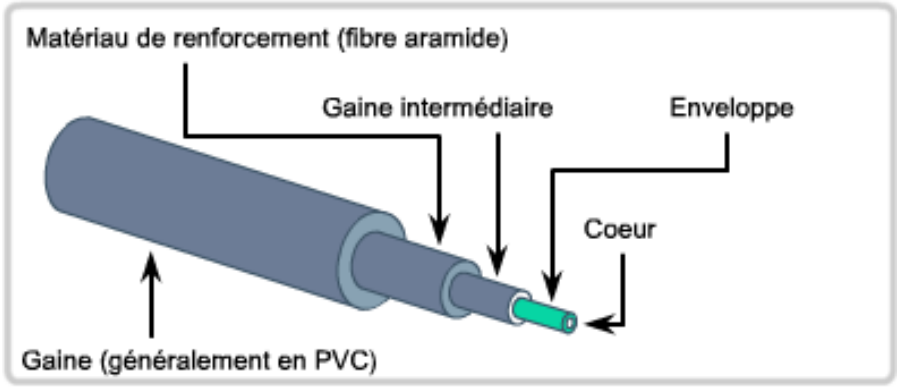
- Les problèmes de mise en œuvre de support en fibre optique comprennent :
  - Un coût plus élevé (généralement) que les supports en cuivre pour la même distance (mais pour une capacité supérieure)
  - Des compétences et matériel différents pour raccorder et joindre l'infrastructure de câble (difficulté de mise en place des coudes)
  - Une manipulation plus délicate que les supports en cuivre

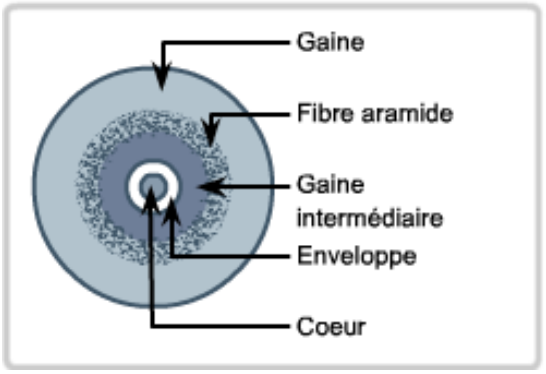
Utilisation

- La fibre est généralement utilisée par les opérateur télécom pour interconnecter des sites distant ayant une demande élevée de bande passante
- En entreprise les fibres peuvent être utilisés en réseaux fédérateur (réseau reliant plusieurs Switch)

Composition de la fibre

- La fibre en aramide vise à empêcher la perte de lumière





Communication full duplex

- La lumière se propage dans un seul sens
- Pour une communication bidirectionnelle il faut deux fibres

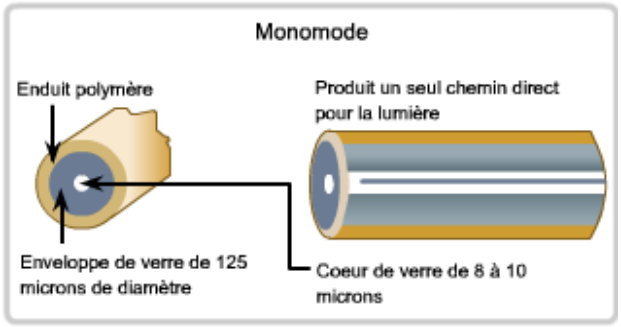
- Les connecteurs de fibre peuvent connecter deux fibres à la fois

Génération du signal optique

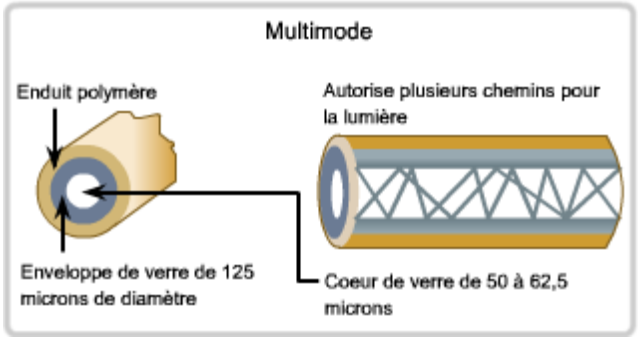
- Des lasers ou des diodes électroluminescentes (DEL) ou (LED en anglais) génèrent les impulsions lumineuses pour représenter les bits
- Des photodiodes détectent les impulsions lumineuses et les convertissent en tensions qui peuvent ensuite être reconstituées en trames de données.

Fibre monomode et fibre multimode

- La fibre monomode transporte un seul signal lumineux généré par un laser qui voyage au centre de la fibre => parcourt de très longues distances



- La fibre multimode utilise les LEDs qui créent plusieurs ondes qui entrent dans la fibre avec différentes angles=> plus de temps de traversée et risque de distorsion modale (dispersion des ondes)



Support sans fil

- Les ondes électromagnétiques qui circulent dans l'air sont utilisées pour envoyer les bits
- Les bits sont représentés par l'amplitude, la fréquence ou la phase d'une onde (ou une combinaison de ces grandeurs)
- Les interférences et la présence d'obstacle entre l'émetteur et le récepteur limitent les performances des réseaux sans fil

Catégories de réseaux sans fil

- Catégories de réseaux sans fil basées sur la portée:
  - WPAN: wireless personal area networks (ex: bluetouth basée sur la norme IEEE802.15)
  - WLAN: wireless local area networks (ex: WiFi basé sur la norme IEEE802.11)
  - WMAN: wireless metropolitain networks (ex: WiMAX basé sur la norme IEEE802.16)
  - WWAN: wireless wide area networks (ex: UMTS basé sur des normes de ITU)

La couche liaison de données: Ethernet

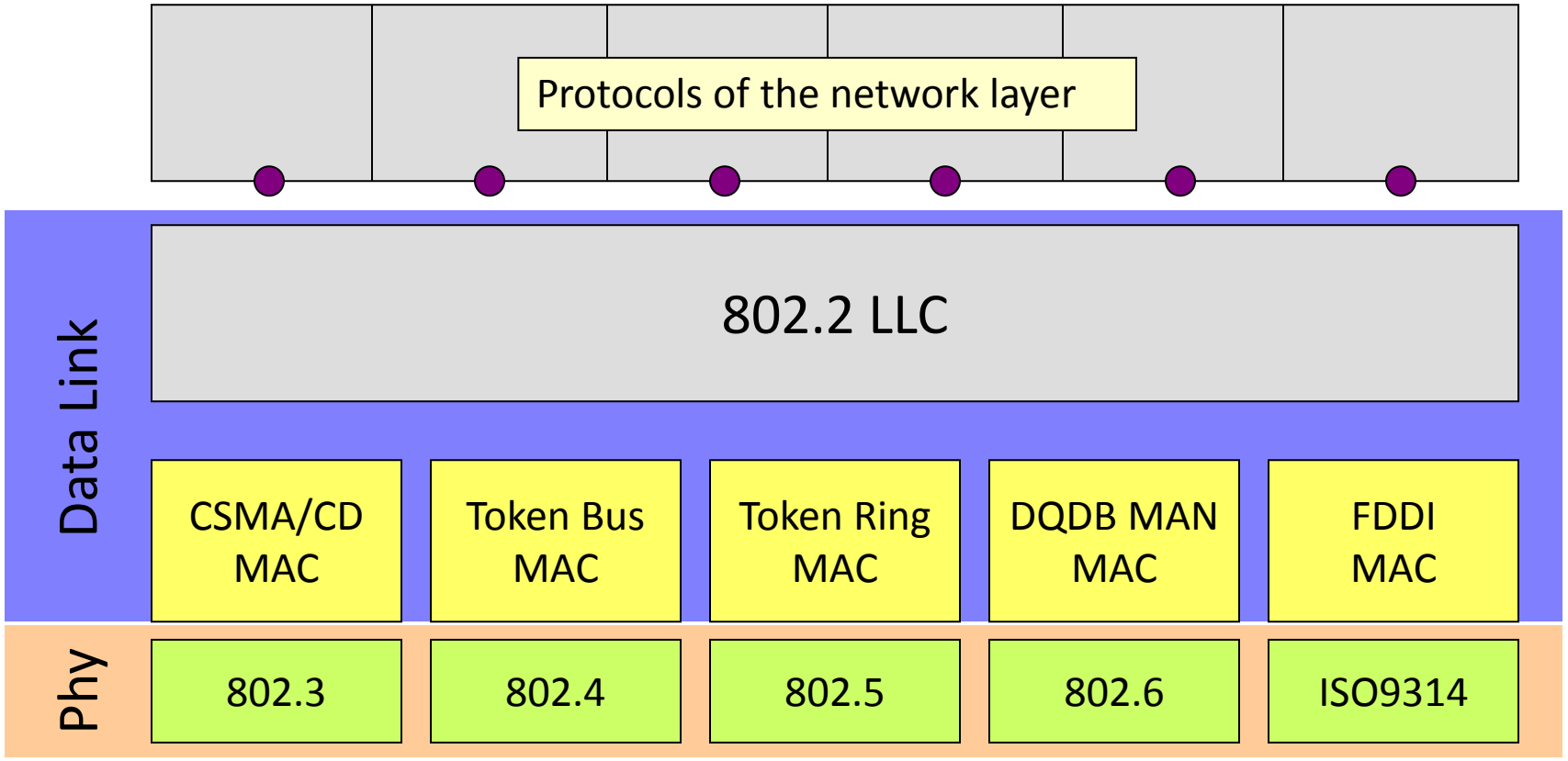
Réseau Ethernet

- Ethernet implémente la couche liaison de donnée et physique
- Standardisé par IEEE (Institute of Electrical and Electronics Engineers)
- La couche liaison de données est divisée en deux sous couche
  - La couche LLC (Logical link control)
  - La couche MAC (Medium Access Control)

La sous couche LLC

- Permet d'établir une connexion logique pour contrôler la transmission d'une machine à l'autre
- Une même sous couche LLC pour plusieurs technologies (token ring, FDDI, ethernet)
- Permet au couches supérieurs d'accéder à différent types de support physique
- Elle basé sur la norme IEEE802.2

La sous couche LLC



La sous couche MAC

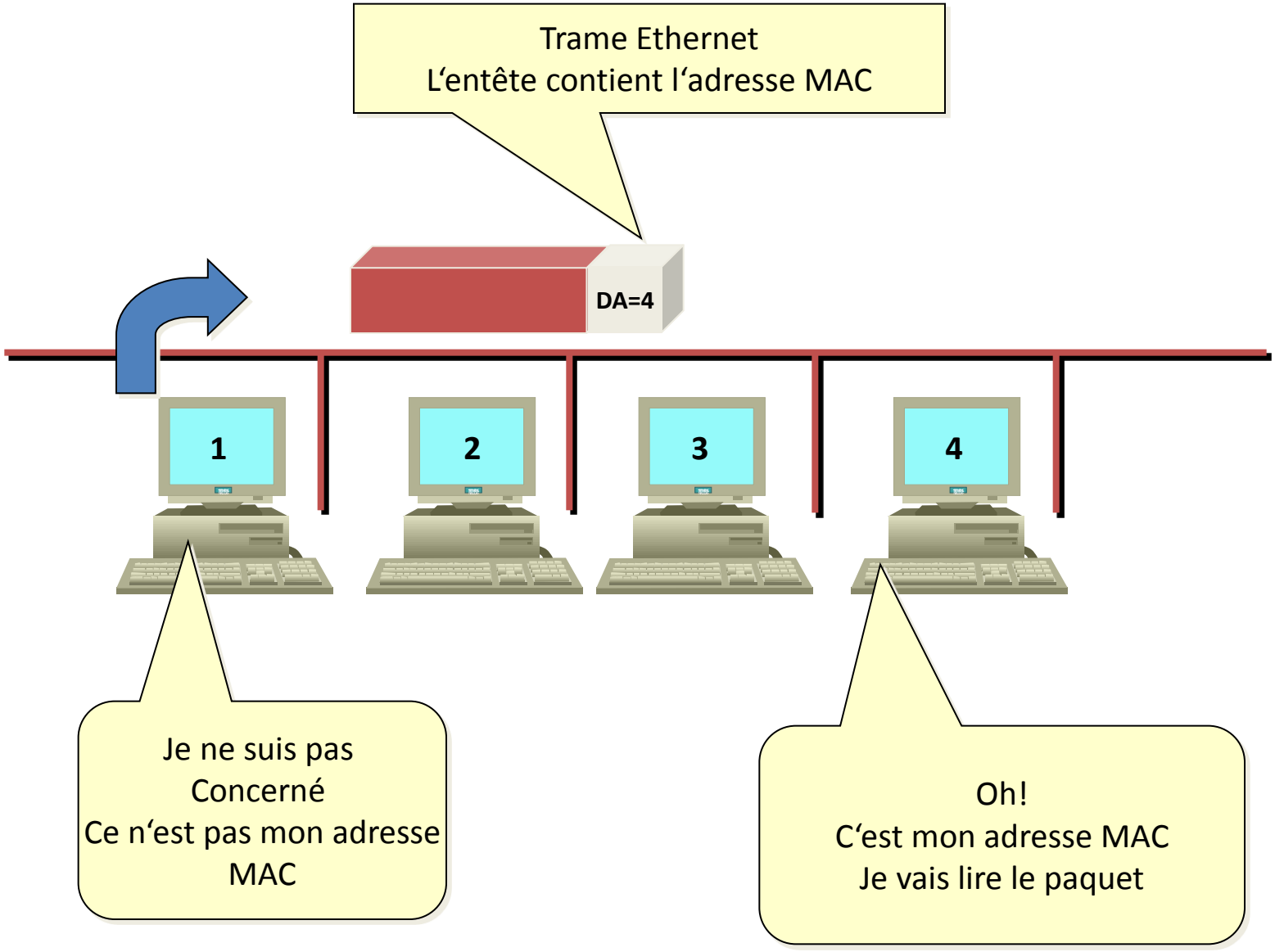
- IEEE 802.3 décrit la couche MAC et Physique
- Basé sur la méthode d'accès CSMA/CD (Carrier Sense Multiple Access / Collision Detection)
- Cette méthode organise l'acces à un support partagé => topologie logique bus (utilisation d'un hub)

adresse MAC

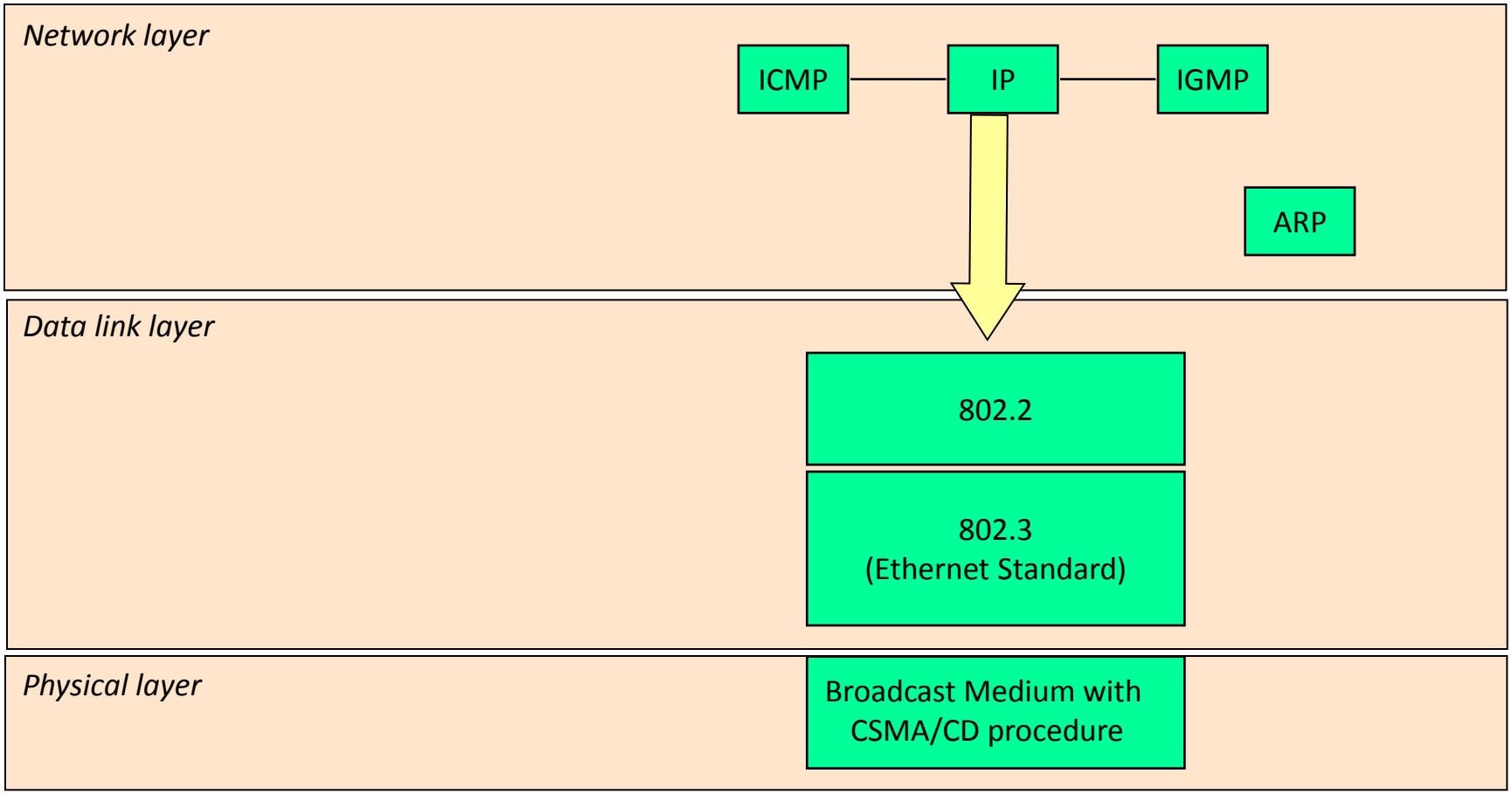
- Une adresse MAC est attribuée par le constructeur de la carte réseau
- Elle se compose de 48 bit
- 3 octets désigne le constructeur et les 3 autres définie l'équipement
- Une adresse MAC est unique dans la monde
- Ex: 78-2B-CB-ED-93-9E (Dell)
- Adresse de diffusion: FF-FF-FF-FF-FF-FF

Transmission d’une trame Ethernet

- Ethernet a une topologie bus (étoile avec un switch)
- La trame transite par toutes les stations
- La station vérifie l’adresse MAC si l’adresse ne la concerne pas l’ignore


Trame Ethernet
L'entête contient l'adresse MAC
DA=4
1
2
3
4
Je ne suis pas
Concerné
Ce n'est pas mon adresse
MAC
Oh!
C'est mon adresse MAC
Je vais lire le paquet

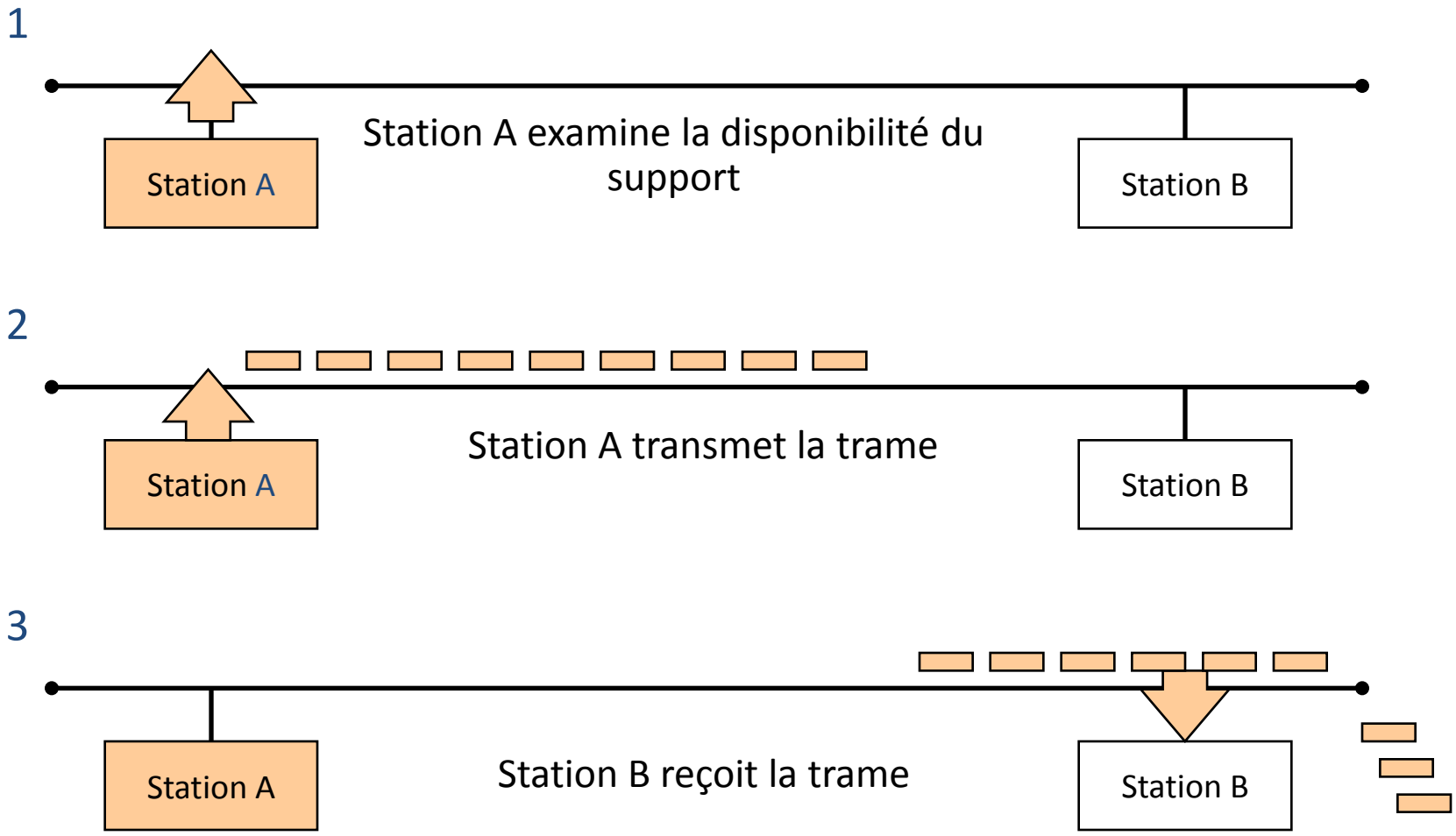
Positionnement de Ethernet



CSMA/CD

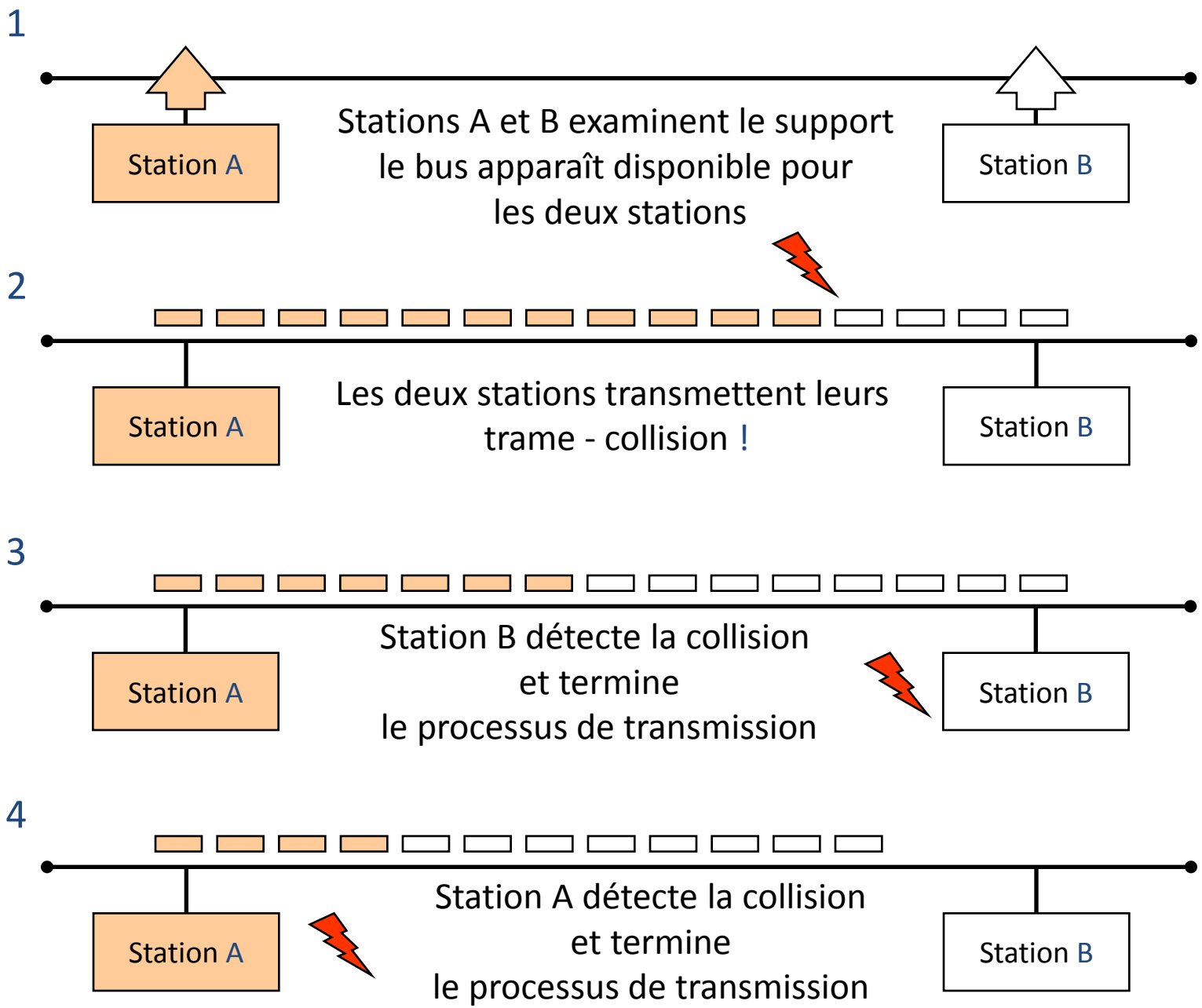
- Un réseau Ethernet est un réseau partagé
- Une seule station peut utiliser le support à la fois
- L'accès multiple doit être réglementé pour éviter les **collisions**
- La station doit d'abord écouter la porteuse sur le media (it senses the carrier)
- Si le media est vide (porteuse vide)=> transmission

Ethernet – CSMA/CD



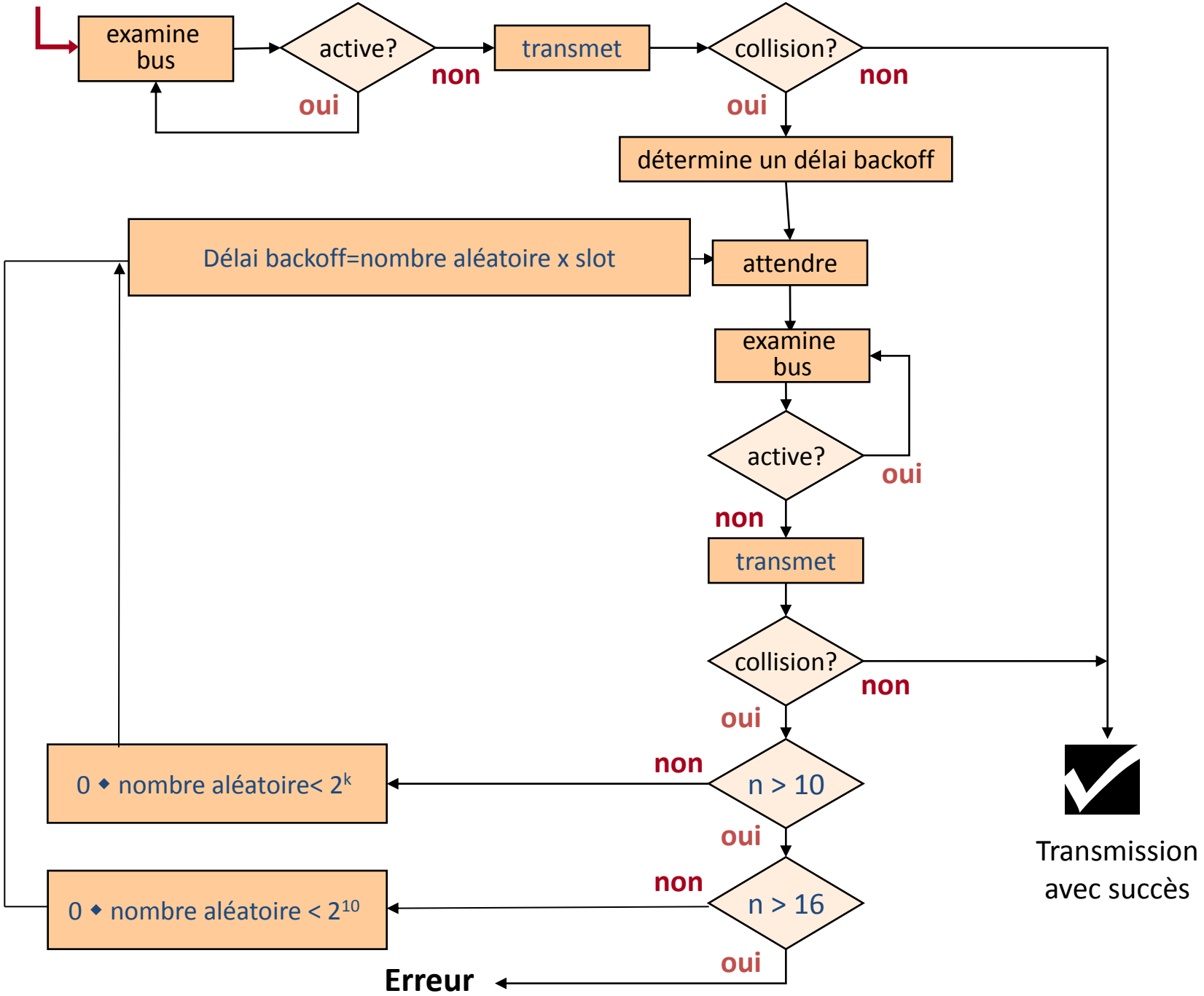
Détection de collision et backoff

- La station transmet la trame et reste à l'écoute
- Si deux stations transmettent en même temps => collision (pas de chef d'orchestre)
- La collision est détecté par toutes les stations du réseaux
- Une collision = quantité anormal d'énergie dans le support
- Gestion de la contention par un système de backoff (retransmettre plus tard)


1
Station A
Stations A et B examinent le support
le bus apparaît disponible pour
les deux stations
Station B
2
Station A
Les deux stations transmettent leurs
trame - collision !
Station B
3
Station A
Station B détecte la collision
et termine
le processus de transmission
Station B
4
Station A
Station A détecte la collision
et termine
le processus de transmission
Station B

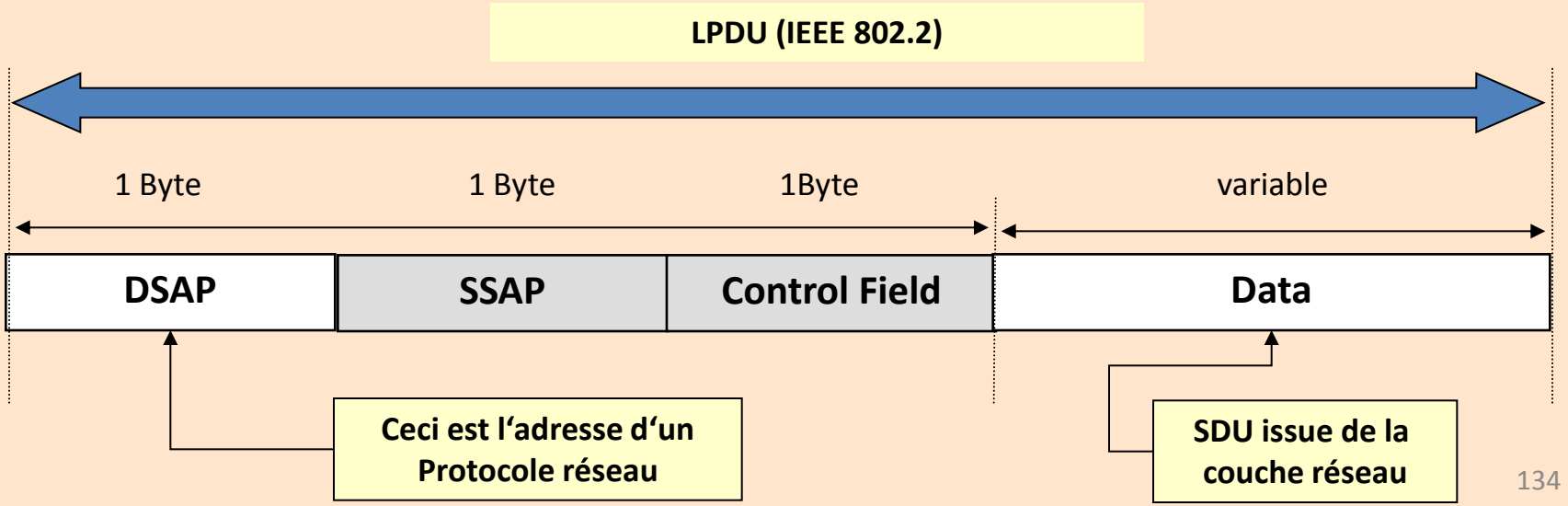
Algorithme de backoff

- Pour minimiser les chances d'une deuxième collision l'une des deux stations doit retarder sa transmission
- Le temps d'attente suit l'algorithme suivant:
  - soit ***n*** le nombre de collisions.
  - Le délai total du backoff = nombre aléatoire * la période d'un slot
  - Nombre aléatoire(n): = $\{ r \mid 0 \leq r < 2^k \ ; k = \min(\boldsymbol{n}, 10) \}$
- Plus la trame entre en collision plus le paquet tarde à être transmis => baisse du débit
- Plus il y a de stations qui transmettent des données plus il y aura de collision


examine bus
active?
non
oui
transmet
collision?
non
oui
détermine un délai backoff
Délai backoff=nombre aléatoire x slot
attendre
examine bus
active?
oui
non
transmet
collision?
non
oui
0 ◆ nombre aléatoire< 2k
non
n > 10
oui
0 ◆ nombre aléatoire < 2^10
non
n > 16
oui
Erreur
Transmission avec succès

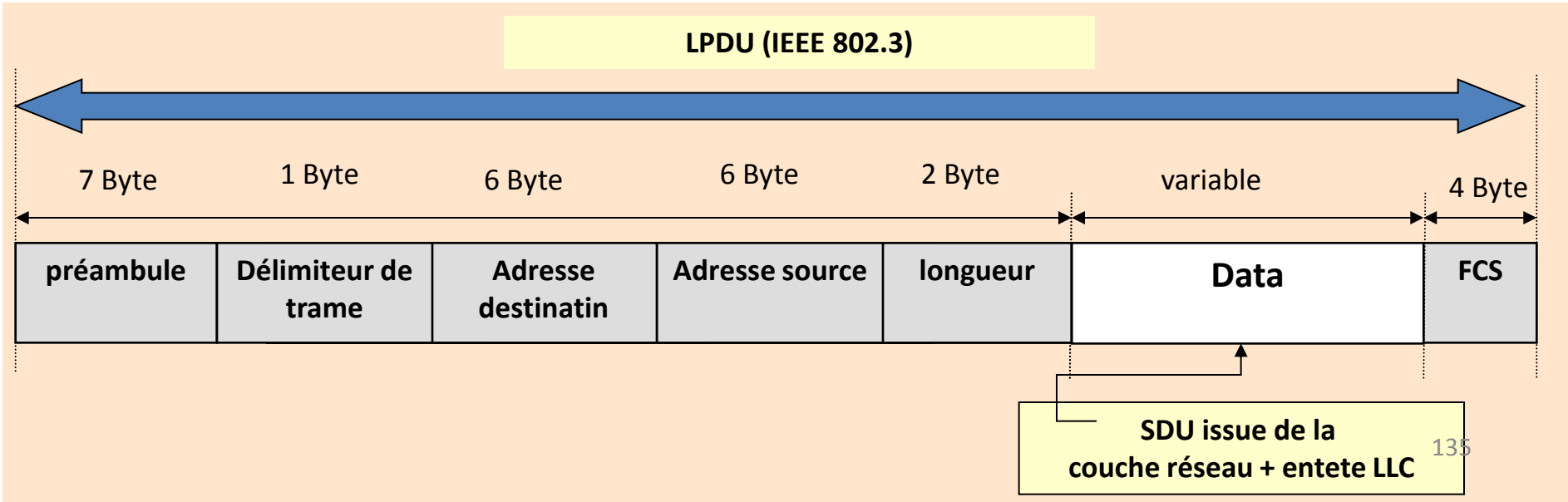
Entête LLC (802.2)

- LPDU (LLC protocol data unit) est composé de:
  - DSAP: destination SAP
  - SSAP: source SAP
  - Control field
  - Data: SDU de la couche réseau



Entête MAC (802.3)

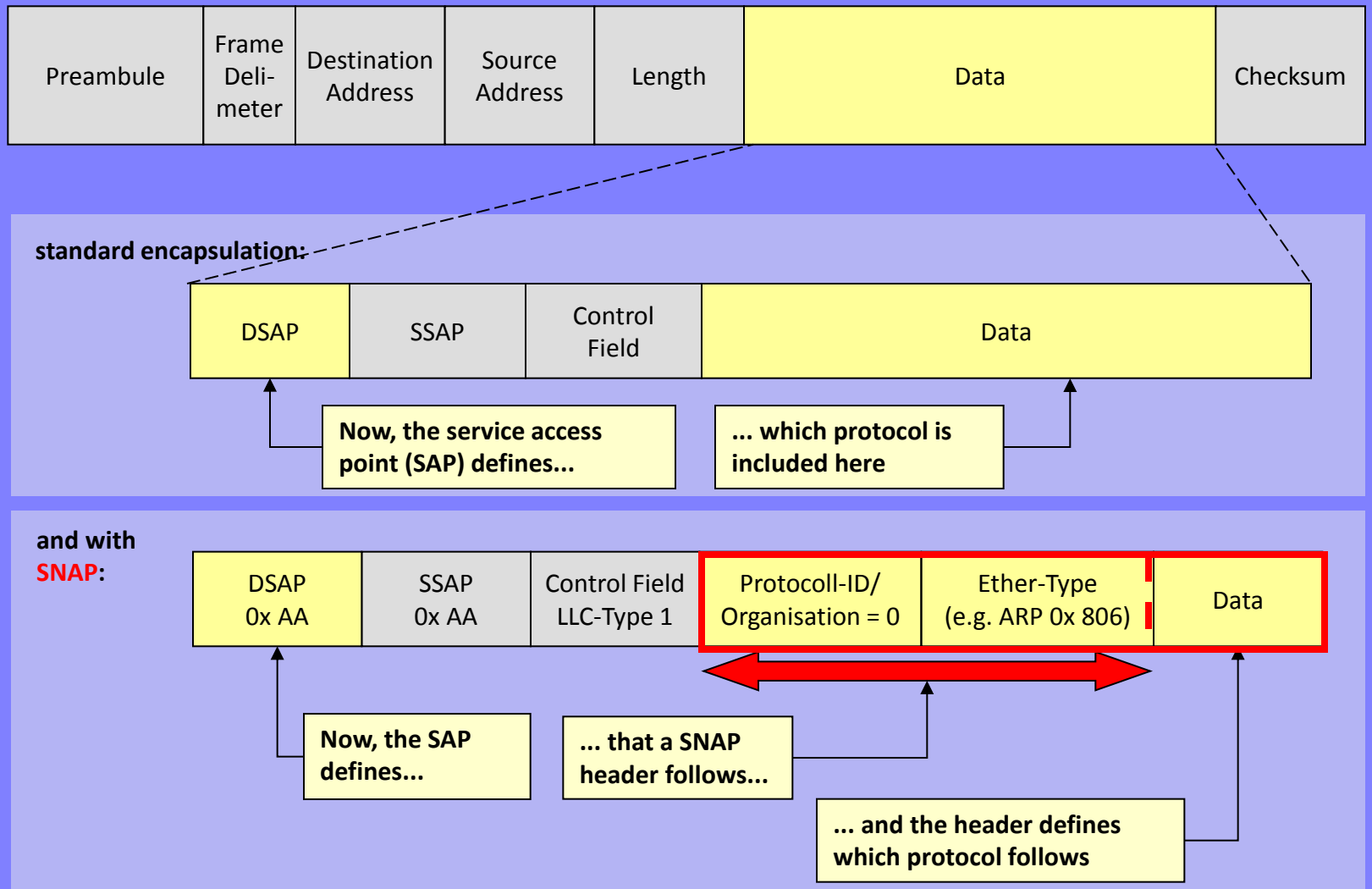
- La trame 802.3 est composé de:
  - Préambule: sert à synchroniser la trame
  - Délimiteur de trame : représente la limite réelle de la trame
  - Adresse destination: adresse MAC de la destination de la trame
  - Adresse source: adresse MAC de la source de la trame
  - Longueur: spécifie la longueur du champ data
  - FCS: frame check séquence (contrôle d'erreur)



SNAP

- Un octet DSAP n’est pas suffisant pour identifier tout les protocoles réseaux existant
- SNAP (Sub Network Access Protocol) permet d’identifier une variété de protocoles
- Le protocole réseau à transmettre est inséré dans une trame SNAP
- elle contient 5 octet: 3 consacrés au constructeur et 2 octets pour identifier le protocole réseau

Ethernet Frame (IEEE 802.3, 802.2) with LLC

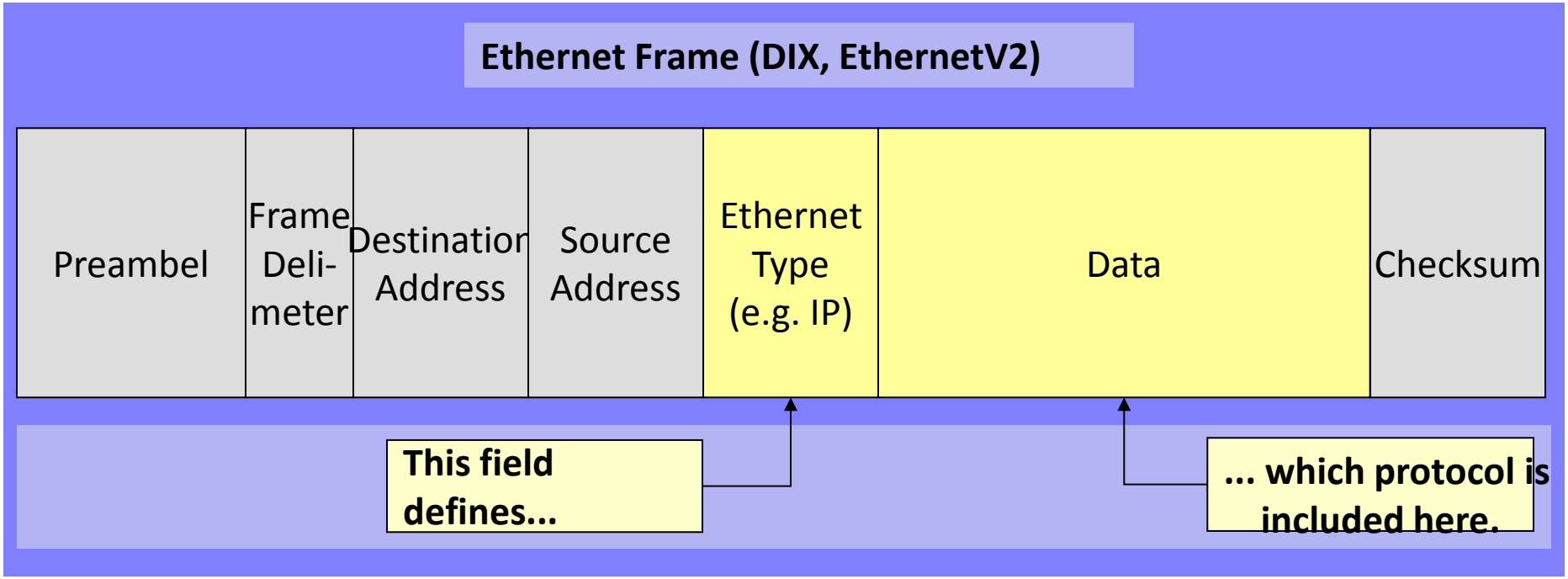


Variantes Ethernet

- Il existe deux variantes du protocole Ethernet:
  - Variante 1: c'est la norme standard de l'IEEE 802.2 et 802.3
  - Variante 2: appelé aussi Ethernet 2 est la propriété de Digital-Intel-Xerox (DIX)
  - La différence entre les deux est dans la structure de la trame
  - Le champ longueur contient la taille de la trame en Eth 1, en Eth 2 il contient le type du protocole réseau
  - Deux stations de différents types ne peuvent pas communique mais peuvent faire partie du même réseau

ETHERNET II

- Le champ longueur de la trame 802.3 est remplacé par le DSAP sur 2 octet (Ether type)
- La sous couche LLC est supprimée

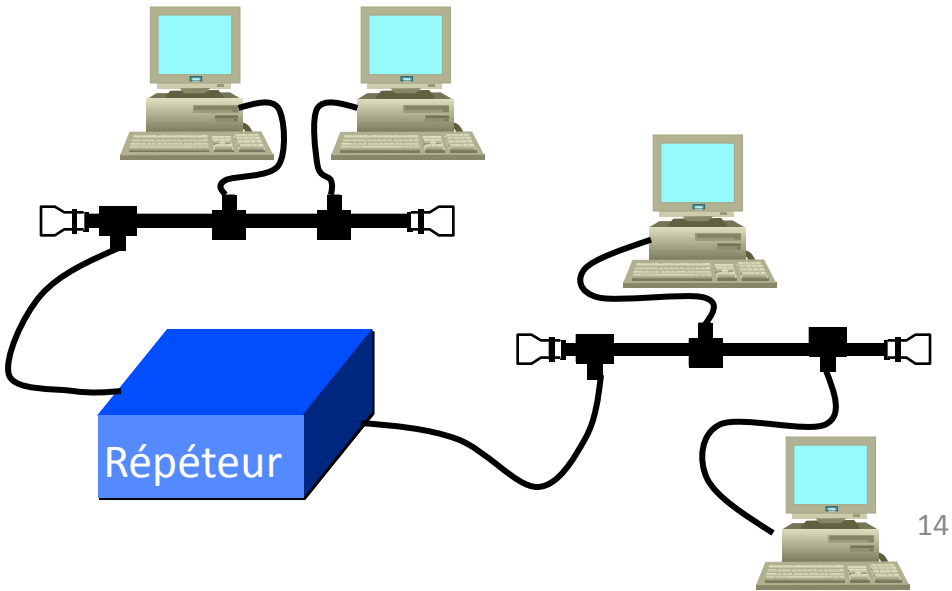


Equipements d’interconnexion

Répéteur

- Un répéteur est un équipement de couche1 en half duplex
- Les segments réseau Ethernet sont de courtes longueurs <1km
- Un répéteur permet de relier deux segments d'un réseau Ethernet => élargir le réseau local
- Amplifier le signal après affaiblissement

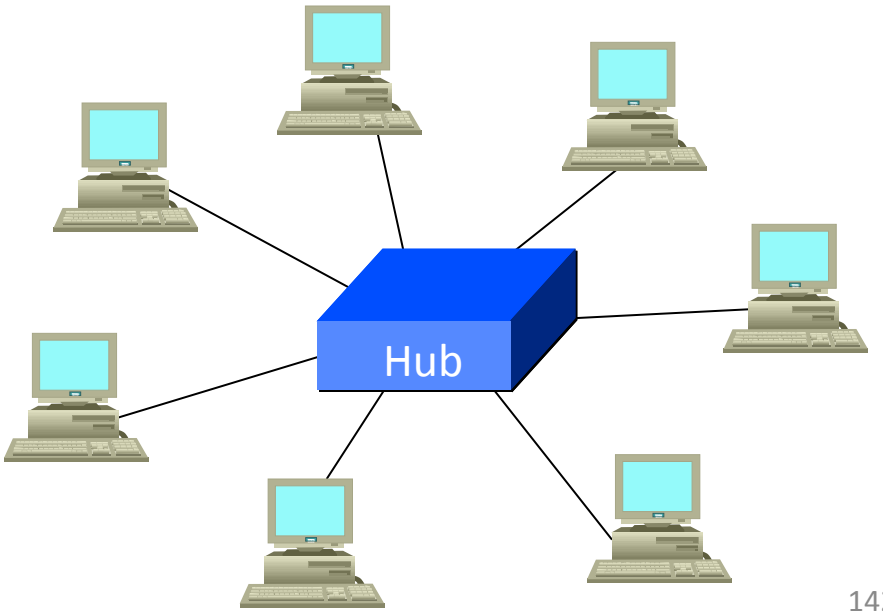
un répéteur relie les segements ensemble



Hub

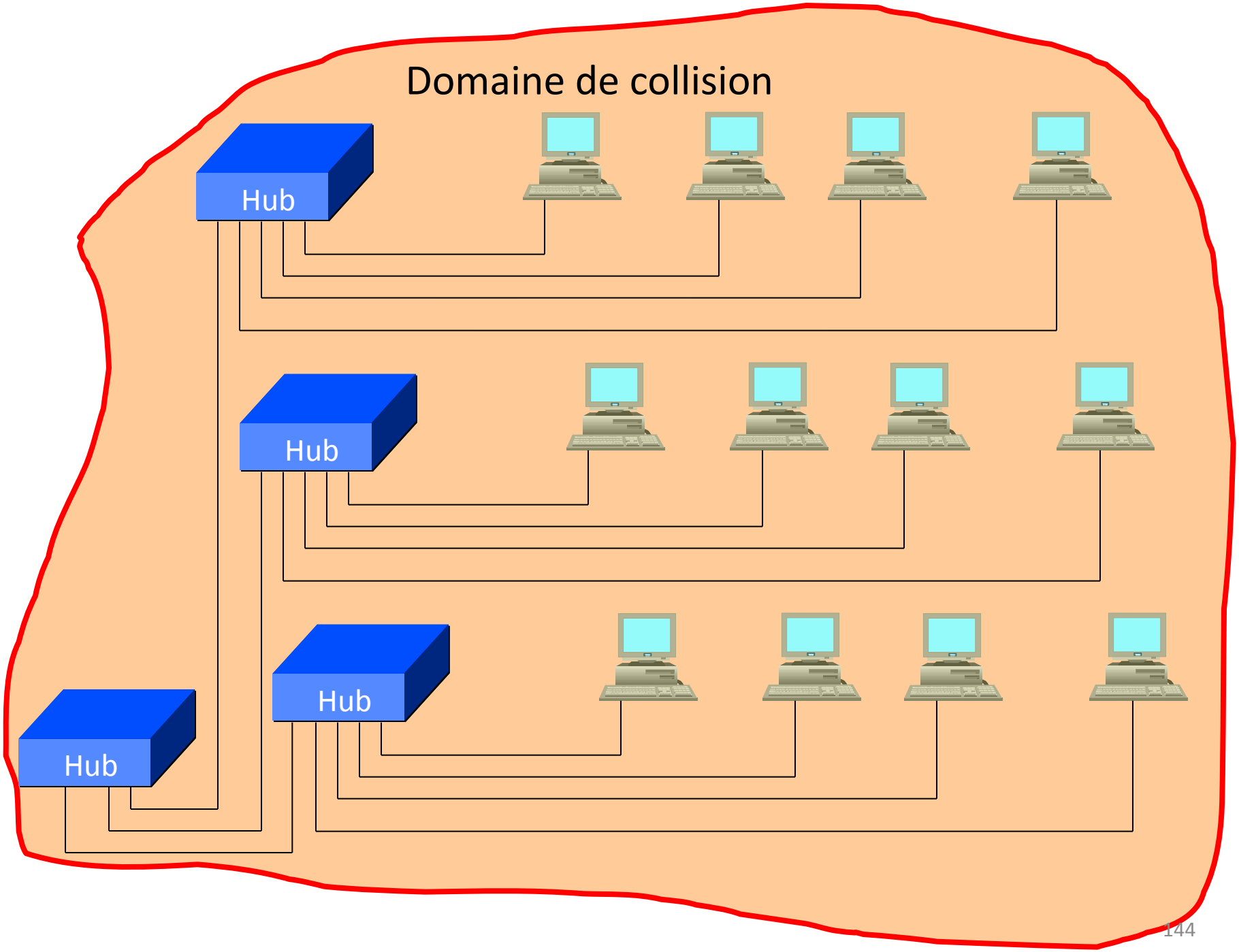
- Un hub a les mêmes caractéristique qu'un répéteur mais peut relier plusieurs machines et segments
- Un hub établit une topologies en étoile physique mais la topologies logique reste toujours un bus
- PS: les hubs ont largement remplacés les répéteurs

un répéteur avec plusiers ports est utilisé comme un hub (topologie physique en étoile)



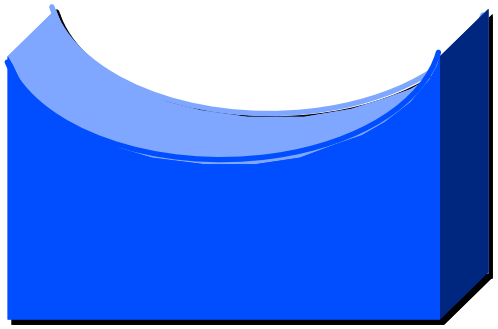
Domaine de collision

- **Domaine de collision**: est un seul réseau CSMA/CD où toutes les stations peuvent rentrer en collision
- Répéteur et hub connectent des domaines de collision ensemble
- Seuls les équipements de couche 2 ou plus peuvent terminer un domaine de collision


Domaine de collision
Hub
Hub
Hub
Hub

Interconnexion avec un pont

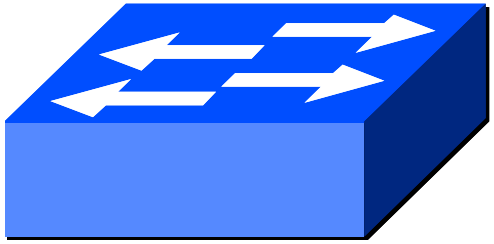
- Un pont permet de segmenter un grand réseau LAN



- Un pont est un équipement de couche 2
- Il dispose de deux ports pour passer les trames d'un réseau à un autre (pont)

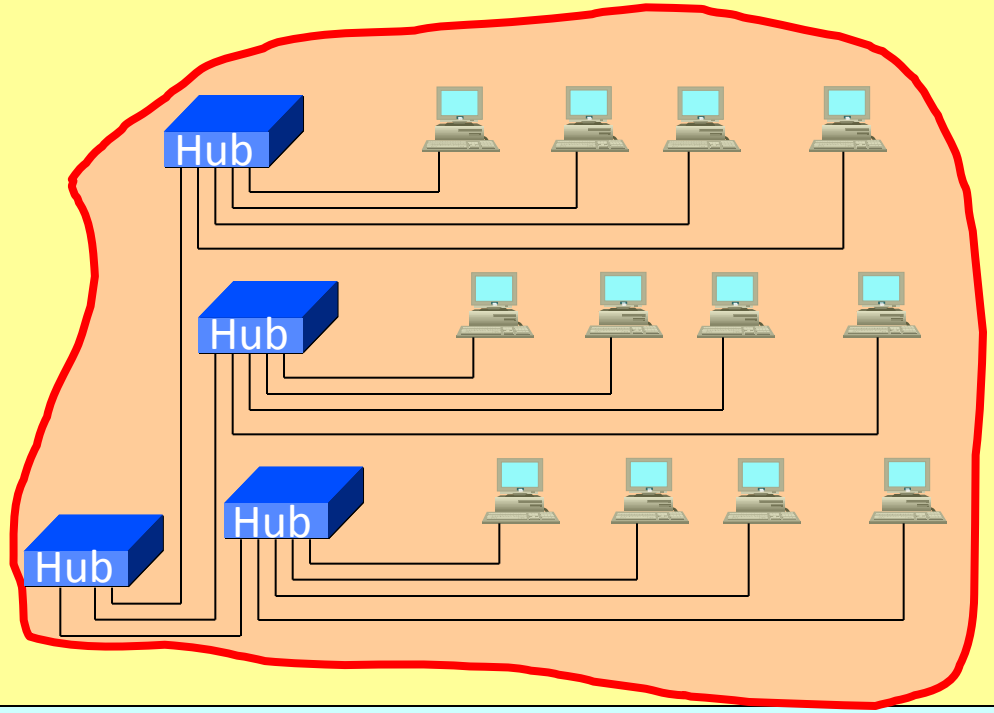
Switch

- Un switch fait la même fonction qu'un pont mais dispose de plusieurs port



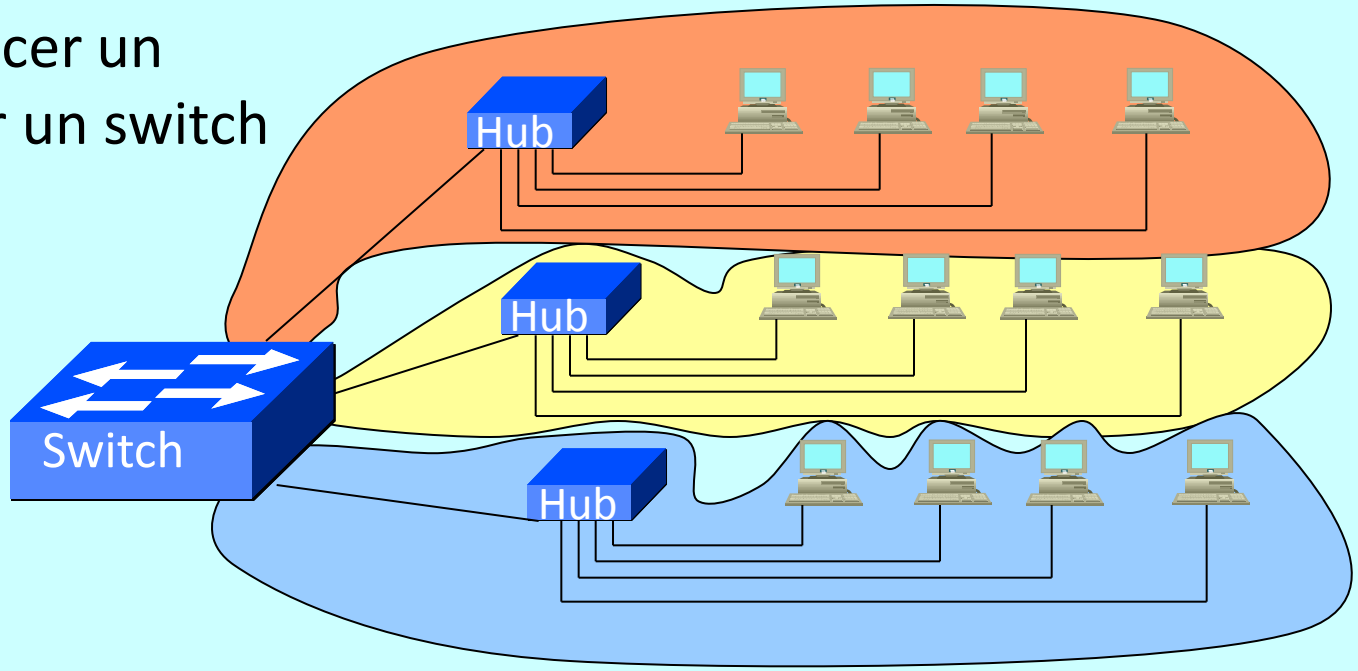
- Changement d'un hub par un switch
  - Communication Full duplex
  - Pas de collision
- Les hub sont largement changés par des switchs surtout avec la baisse des prix

Utilisation de hubs seulement



Un domaine de collision

Remplacer un hub par un switch



3 Domaines De collision

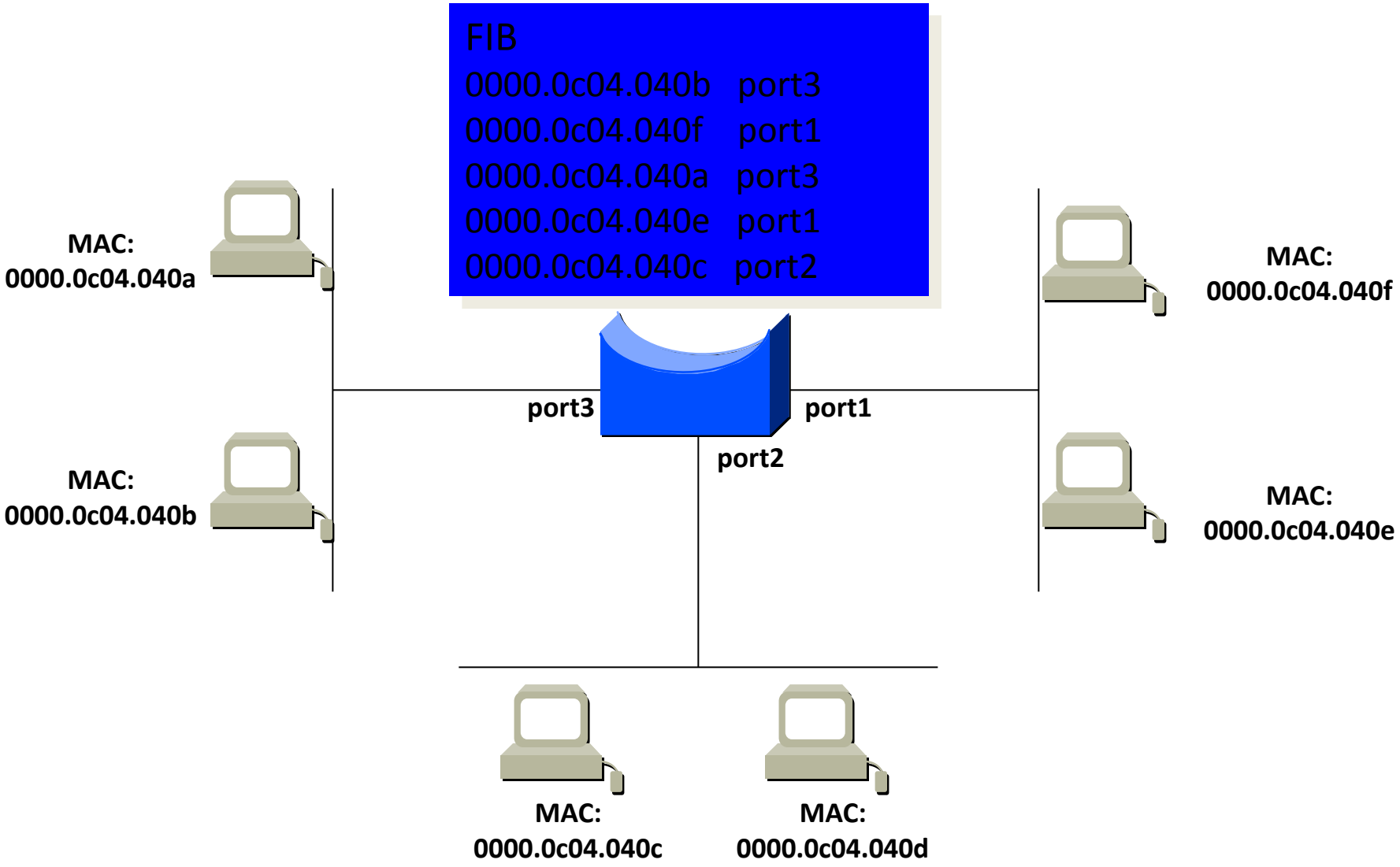
Fonctionnement

- Deux types de switch:
  - Cut through: seul l'adresse destination est lue => plus rapide
  - Store and forward: toute la trame est lue => permet de ne pas propager les erreurs
- Le switch transfère les trames en se basant sur les adresse mac des stations
- Mais il doit d'abord établir la correspondance port adresse MAC

Forwarding Information Base

- Apprentissage des adresse MAC: quand le switch (ou pont) est allumé, il commence par regarder l'adresse MAC source de la trame
- Inscrit l'adresse MAC et le port par lequel la trame est reçu
- Constitue une table de correspondance appelée FIB (Forwarding Information Base)
- Consulte la base pour faire un acheminement (commutation) de trame
- Si aucune correspondance n'est trouvé la trame est diffusée sur tous les ports

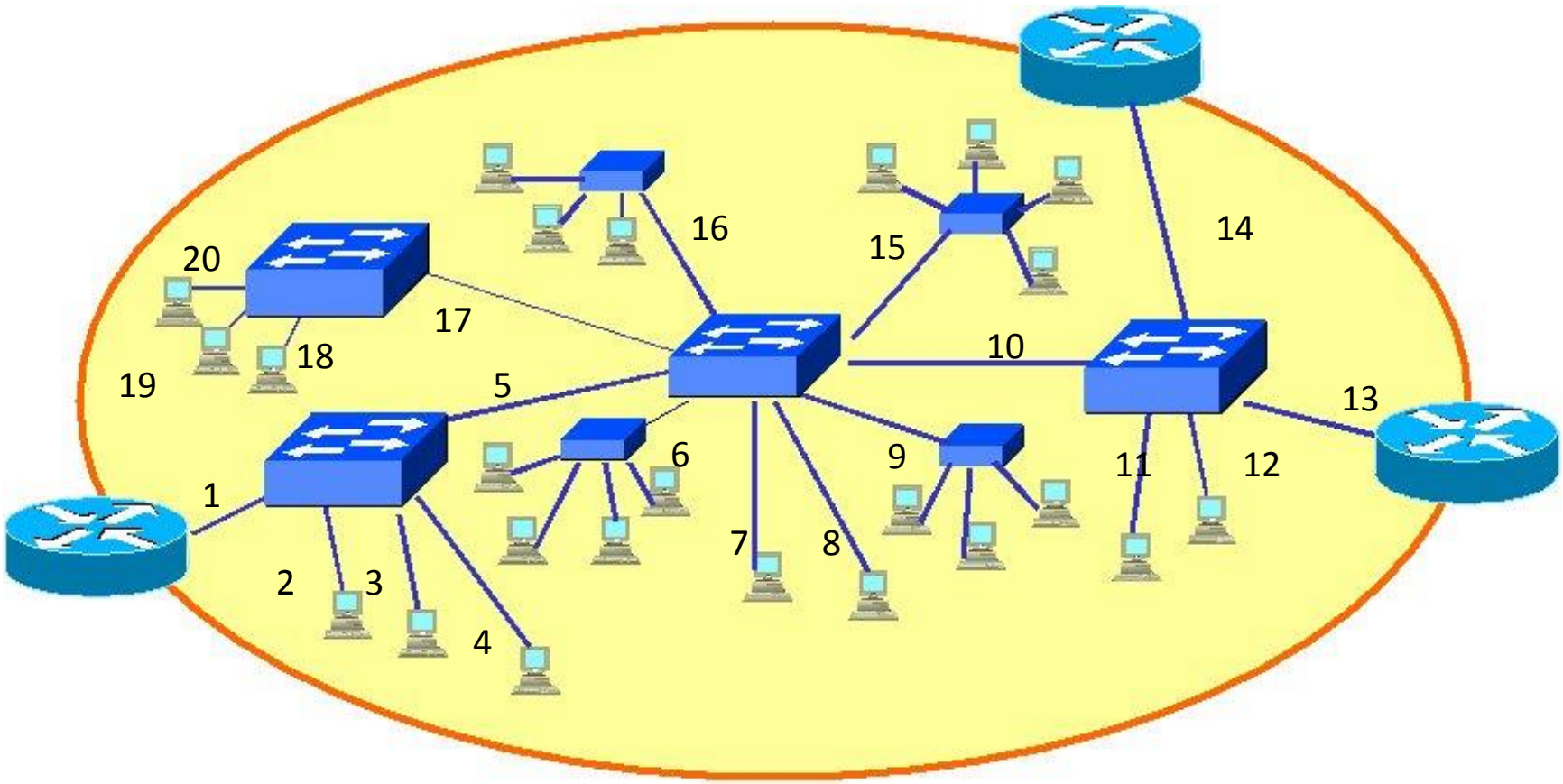
Apprentissage des adresses



Broadcast

- Une adresse Broadcast est une adresse de diffusion vers toutes les stations du réseau
- le switch diffuse une trame avec une adresse de destination broadcast vers tout les autres port sauf le port par lequel il la reçu (pareil pour un pont)
- Le switch se comporte comme un hub lorsqu'il s'agit d'une adresse broadcast on parle domaine de diffusion
- Seul un routeur (équipement de niveau 3) bloque les broadcasts

combien y-a-t-il de domaines
de collision et de diffusion dans ce réseau ?



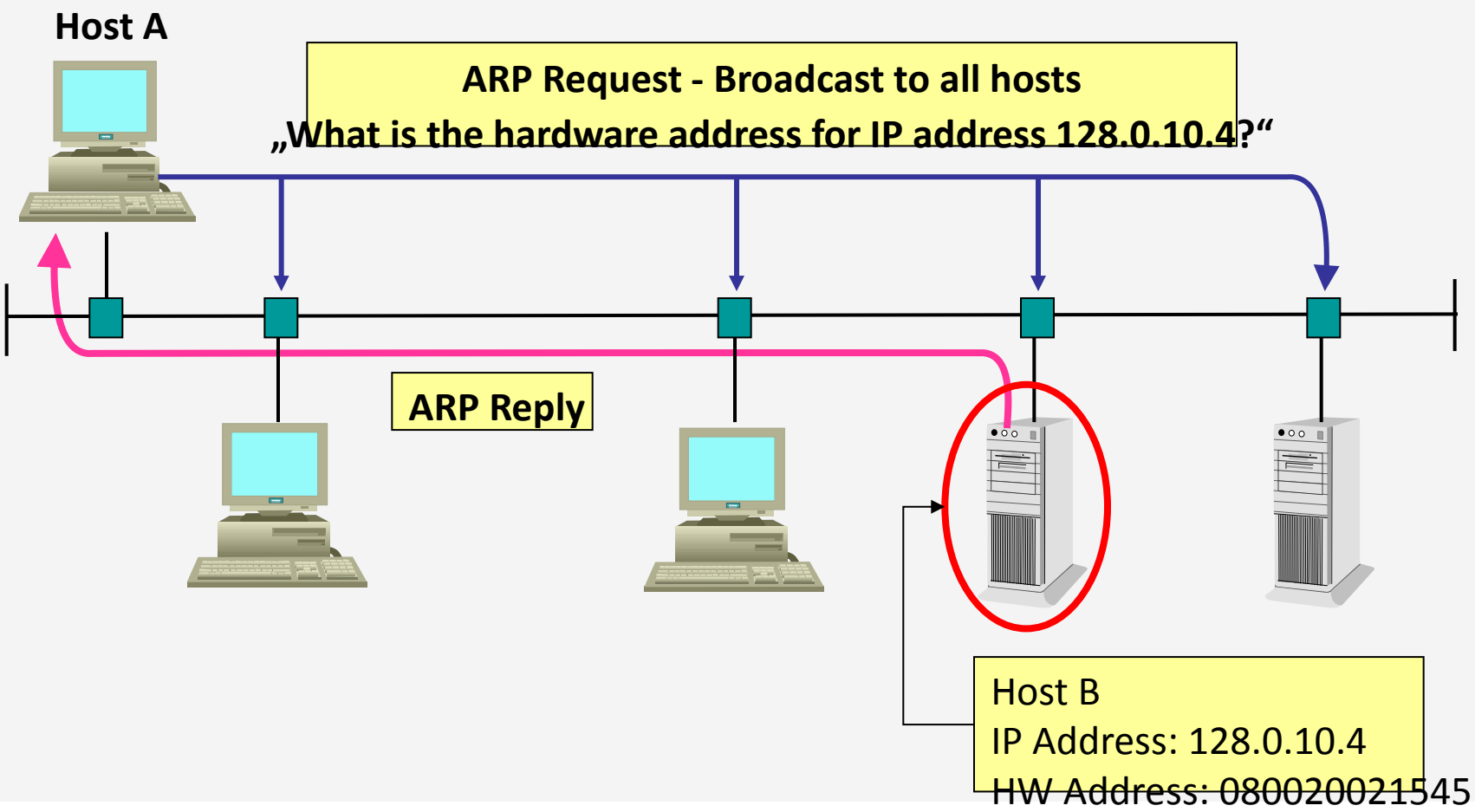
Adresse Resolution Protocol

- Une trame ne peut être émise sur le lien si elle ne dispose pas de touts les champs de la trame MAC
- Il est difficile de retenir une adresse IP de 32 bit encore moins une adresse Mac de 48 bit
- Les humains se rappellent plus des noms de machines
  - DNS (domain name system) : nom ⇔ adresse IP
  - ARP: Adresse IP⇔ adresse Mac

Adresse Resolution Protocol

- Le protocole ARP permet de résoudre l'adresse Mac d'une machine sur le réseau étant donné sont adresse IP
- Pour cela une requête ARP en broadcast est diffusée sur le réseau (adresse Mac de destination FF:FF:FF:FF:FF:FF) contenant la question suivante: qui a cette adresse IP?
- La machine avec l'adresse IP recherchée répond en unicast avec un message ARP reply qui contient son adresse Mac

Mécanisme ARP



Cache ARP

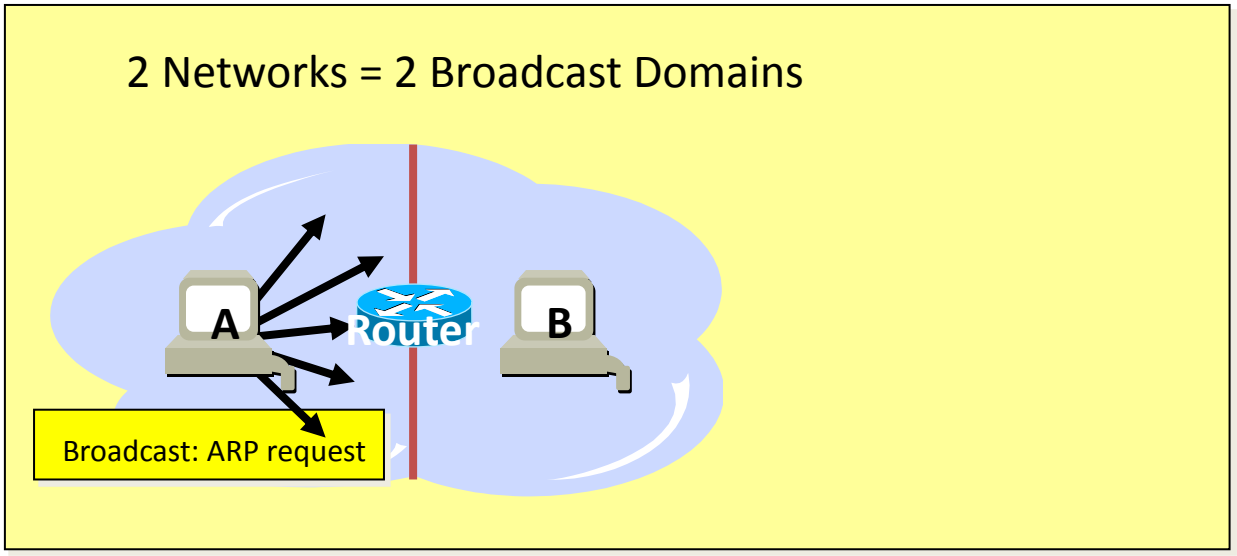
- Pour limiter l'envoi des messages ARP sur le réseau, un cache ARP est entretenu par chaque machine
- La machine consulte d'abord son cache ARP avant d'envoyer une requête ARP
- Le temps de résidence des entrées de la table ARP doit tenir en considération les changements dans le réseau tout en minimisant la fréquence des requêtes ARP
- Windows par exemple supprime une entrée au bout de 2 minutes, si la même entrée est sollicitée avant sa suppression le temps de suppression devient 10 minutes

ARP et sécurité

- Le protocole ARP présente une faille de sécurité: ARP spoofing
- Un utilisateur mal intentionné peut répondre à des requêtes ARP pour prétendre être le détenteur d'une adresse IP pour pouvoir détourner le trafic
- Pour limiter ce risque on peut entrer des associations ARP manuellement mais c'est une tache qui n'est pas facile avec un nombre important de machines, il faut aussi sécuriser les ports

Proxy ARP

- Avec la subdivision en sous réseaux le routeur bloque les diffusions
- la communication entre la machine A et B se passe à travers le routeur :
  - Soit en indiquant un chemin par défaut à la machine A (la route par défaut indique l'adresse du routeur)
  - Soit en envoyant un ARP request à la machine B qui sera intercepté par le routeur qui envoie une réponse avec son adresse MAC (Proxy ARP)



Pourquoi les VLANs?

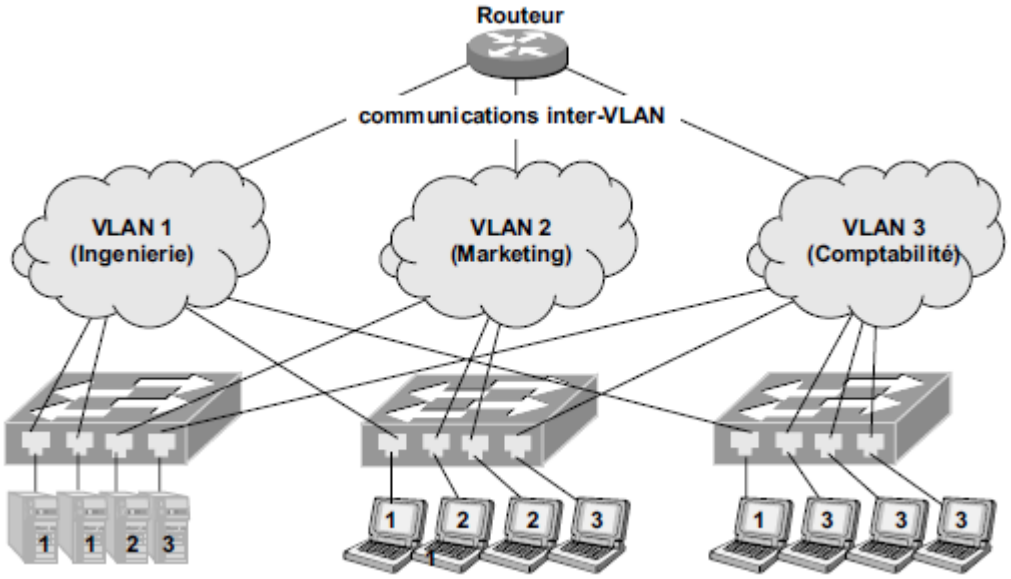
- Les machines d'une entreprise sont regroupées en réseaux selon l'organisation de celle-ci: département, hiérarchie, fonctions…
- Pour pouvoir séparer les réseaux physiquement l'administrateur doit déployer des Switch pour chaque réseau
- Sur le plan opérationnel il est difficile et couteux de dédier des Switch pour les machines d'un même réseau vu la distribution géographique des machines dans l'entreprise
- Il est possible de mettre des machines appartenant à des réseaux différents sur le même Switch mais elles forment un seul domaine de diffusion => diminution de performance + risque de sécurité

Les VLANs

- les VLAN sont des réseaux virtuels qui permettent d'isoler les réseaux logiques même s'ils partagent la même infrastructure (Switch)=> isoler les domaines de diffusion selon l'appartenance logique des machines
- Ils séparent la distribution physique des réseaux de leur organisation logique
- Exemple: dans un même local le PC du PDG et le PC de son assistante sont connectées sur le même Switch mais ils appartiennent à des réseaux (domaine de diffusion différent)

Communication entre VLANs

- Un PC du VLAN 1 ne peut communiquer directement que avec un autre PC du VLAN 1 (y compris les trames de broadcast)
- La communication inter VLAN passe par le routeur



Types de VLAN

- Vlan statique: attribution du VLAN au port du Switch
- Vlan dynamique: attribution du VLAN selon l'adresse MAC ou l'adresse IP de la machine
- Un VLAN est identifié par un ID de 1 à 1005
- Il existe deux types de port:
  - Un port d'acces qui appartient à un VLAN
  - Un port trunk qui permet de véhiculer des trames de VLAN différents (port connecté avec un autre switch)