Réseaux informatiques

Chapitre 1 – Introduction aux réseaux informatiques

Mustapha Anwar BRAHAMI

ESSA Tlemcen

Objectifs du cours

Pourquoi un réseau ?

- Echanger des informations, supporter et accélérer la communication
- Partager ou vendre des services
- Regrouper des ressources

Pourquoi un cours de réseau en formation d'ingénieur ?

- Vous êtes au contact des réseaux dans votre vie personnelle et professionnelle, et vous devez en être des utilisateurs éclairés
- Vous serez amené en tant que managers à suivre des projets incluant des réseaux informatiques
- Les systèmes d'information (et donc les réseaux) sont le support du métier de toutes les entreprises
- En tant qu'ingénieurs, vous devez étoffer votre culture et votre curiosité scientifique et technique

Objectifs du cours

Dans son ensemble le cours vise les objectifs suivants :

- Comprendre le fonctionnement général des réseaux informatiques.
- Savoir concevoir et analyser une architecture de réseau simple.
- Connaissances de base des protocoles de transmission des couches basses (Transport, Réseau, Liaison et Physique) utilisées dans les réseaux d'ordinateurs et les systèmes d'information en général.
- Comprendre le fonctionnement et les caractéristiques des réseaux locaux (la norme Ethernet notamment).

Contenu du cours

- Introduction et généralités (historique, types de réseaux, topologies …)
- Modèle OSI (différentes couches …)
- Modèle TCP/IP
- Réseaux locaux (norme Ethernet)
- Quelques protocoles (TCP, UDP, Telnet, SSH …)

Références bibliographiques

Ce cours est construit à partir d'un certains nombres de support de cours disponibles sur le net. L'usage de ce composite ne peut être qu'académique :

- DORDOIGNE, J. (2015). *Réseaux informatiques - Notions fondamentales (6ième édition)*. ENI. ISBN : 9782746093928
- LEGRAND, R. (2014). *Notions de base sur les réseaux : 1er module de préparation à la certification CCNA 200-120*. ENI. ISBN : 9782746092136
- DROMARD, D. (2006). *Architecture des réseaux*. Pearson. ISBN : 9782744076640
- LOHIER S. (2010). *Le réseau Internet : des services aux infrastructures*. Dunod. ISBN : 9782100546046
- PARET D. (2012). *Réseaux multiplexés pour systèmes embarqués* : CAN, LIN, FlexRay, Safe by Wire. Dunod. ISBN : 9782100582891
- FERRAND P (2013). *Réseaux*. INSA de Lyon. http://www.ferrand.cc/pdfs/cours_reseaux.pdf
- DUVALLET C (2016). *Architecture et protocoles des réseaux*. Université du Havre. http://litis.univ-lehavre.fr/~duvallet/enseignements/Cours/M1INFO/Reseau/MI-Cours-Reseau-Cours1.pdf
- *Réseaux informatiques, modèle OSI, protocole TCP/IP*. http://info.arqendra.net/Files/_Rsx+OSI+TCPIP_cours.pdf

Définitions

- Un **réseau informatique** est un réseau dont chaque nœud est un système informatique autonome, reliés par un support matériel et logiciel, et qui ont ainsi la possibilité de communiquer entre eux directement ou indirectement.
- En pratique, 2 ordinateurs suffisent pour constituer un réseau informatique

Historique

Quelques grandes étapes de l'histoire des communications

- 1837 - William Cooke, Charles Wheatstone - Télégraphe électrique (Angleterre)
- 1837 - Samuel Morse, Alfred Vail - Télégraphe électrique (États-Unis)
- 1866 - William Gisborne, Cyrus Field - Premier câble transaltantique fonctionnel
- 1876 - Alexandre Graham Bell - Téléphone
- 1901 - Guglielmo Marconi - Première transmission télégraphique sans fil à travers l'atlantique
- 1907 - Édouard Belin - Première transmission d'une photographie
- 1923 - John Baird - Première télévision mécanique

Historique (Internet)

Internet, ça marche

- Mais pourquoi ?
- Simple, intuitif (au moins pour votre/notre génération...)
- Des millions de pages et de services, pour des millions d'utilisateurs simultanés
- Mais en fait, l'Internet, c'est quoi ?

Une technologie jeune

- Le World Wide Web (WWW) n'a que 25 ans
- L'Internet « mondial » en a 30
- En quelques années, Internet a changé la société et s'est rendu presque indispensable
- Et son histoire commence il y a à peine 55 ans

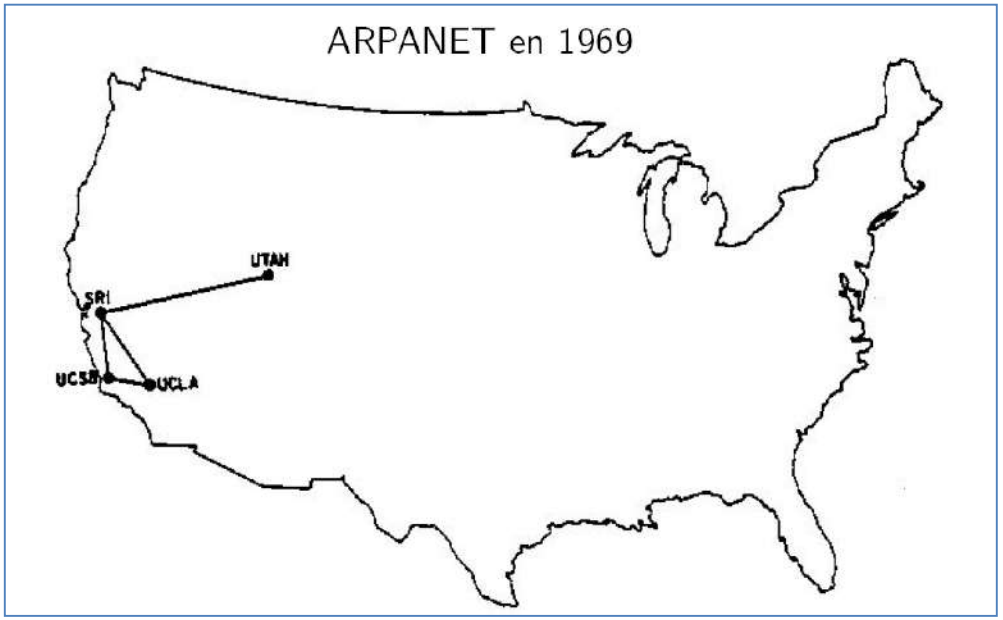
Historique (Internet)

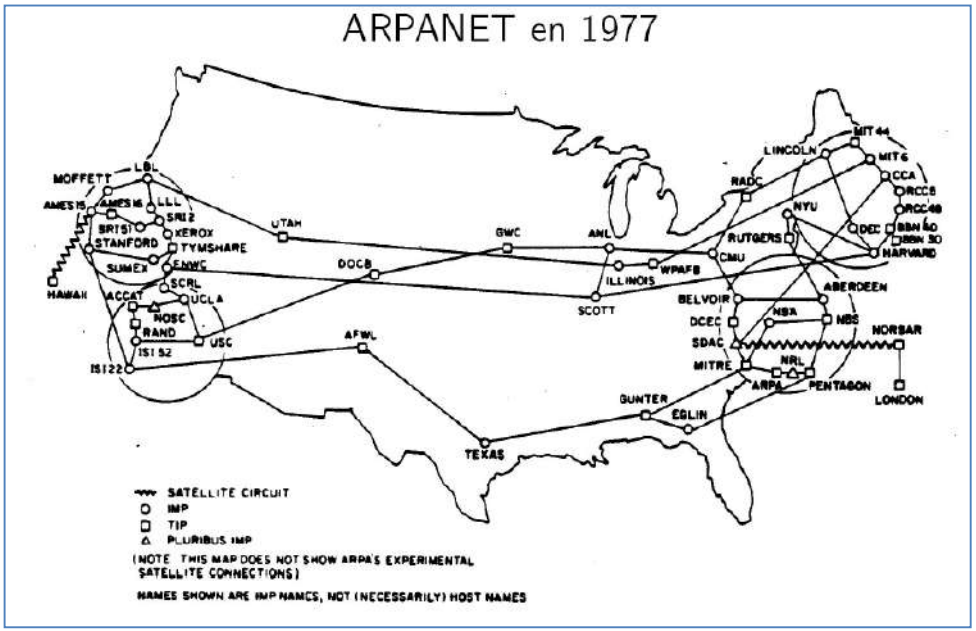
- ***Internet est un nom générique signifiant Interconnexion de Réseaux***
- Le regroupement d'un ensemble de réseaux
  - réseaux locaux (universités et entreprises)
  - réseaux métropolitain (réseau AT de la ville de Tlemcen)
  - réseaux nationaux (réseau AT national)
  - Internet → réseau de tous les réseaux
- Le plus grand réseau informatique du monde relie une communauté mondiale en pleine expansion
- Géré de manière décentralisée

Historique (Internet)

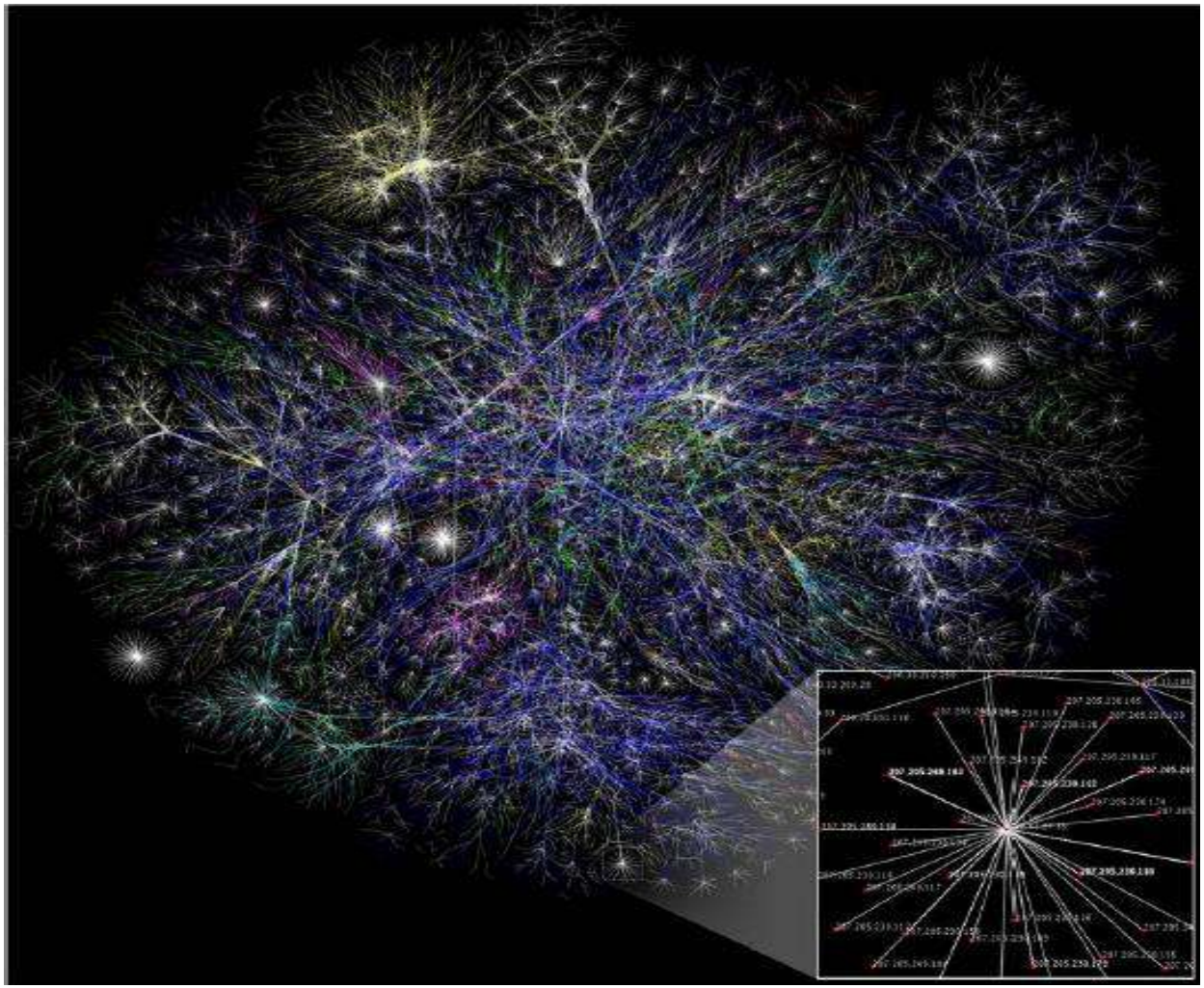
- 1959 - 1968 : Programme ARPA (Advanced Research Projects Agency) :
  - Le ministère américain de la défense décide de lancer un réseau capable de supporter les conséquences d ’un conflit nucléaire
- 1969 : ARPANET, l ’Ancêtre
  - Les universités américaines s’équipent de gros ordinateurs. Elles se connectent au réseau ARPANET
- 1970-1982 : Ouverture sur le Monde
  - Premières connexions avec la Norvège et Londres. Naissance des réseaux UseNet et BitNet
- 1983 : Naissance d’Internet
  - Avec le protocole TCP/IP, tous les réseaux s ’interconnectent
- 1986 : Les autoroutes de l ’information
  - La NSF (National Science Foundation) décide de déployer des superordinateurs afin d ’augmenter le débit d’Internet
- 1987-1992 : Les années d’expansion
  - Les fournisseurs d’accès poursuivent l’expansion du réseau. Par leur biais, les entreprises privés se connectent au réseau

Evolution de l'ARPANET





Internet : réseau des réseaux



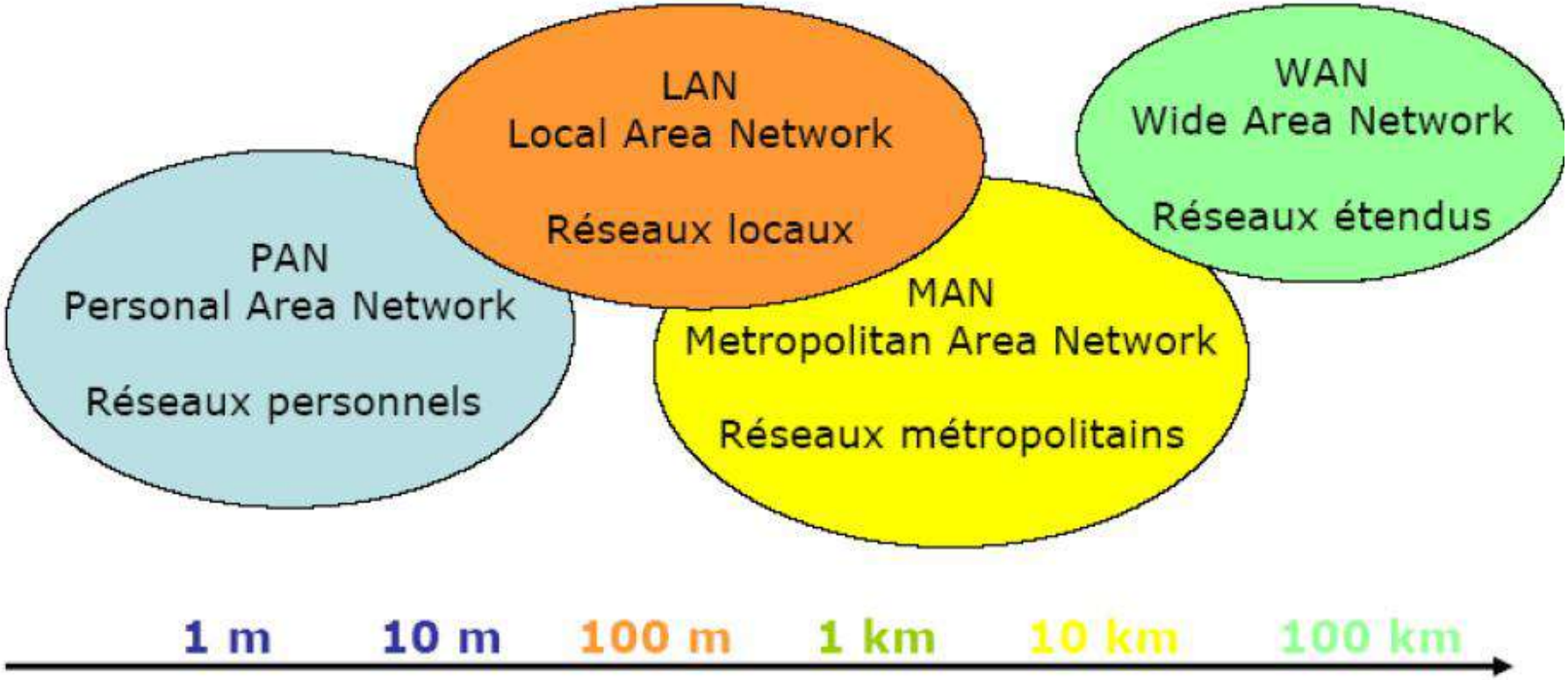
Classification des réseaux

- Pas facile de classer les réseaux car les critères sont multiples
- Distance / Taille
  - Réseaux locaux d'entreprise (LAN)
  - Réseaux de Communauté urbaine ou métropolitains (MAN)
  - Réseaux généraux ou étendus (WAN)
- Topologie
  - Bus
  - Anneau (ex. Token Ring)
  - Etoile (ex. Ethernet)
  - Arbre
  - Maillé (ex. Internet)

Classification des réseaux

- Débit
  - Ethernet 100 Mbits/s
  - ATM jusqu'à 622 Mbits/s
- Mode de transmission
  - filaire (ex. Ethernet)
  - sans fil (ex. Wifi, GSM)
  - fibre (ex. FDDI, ATM)

Classification (Distance – étendue géographique)



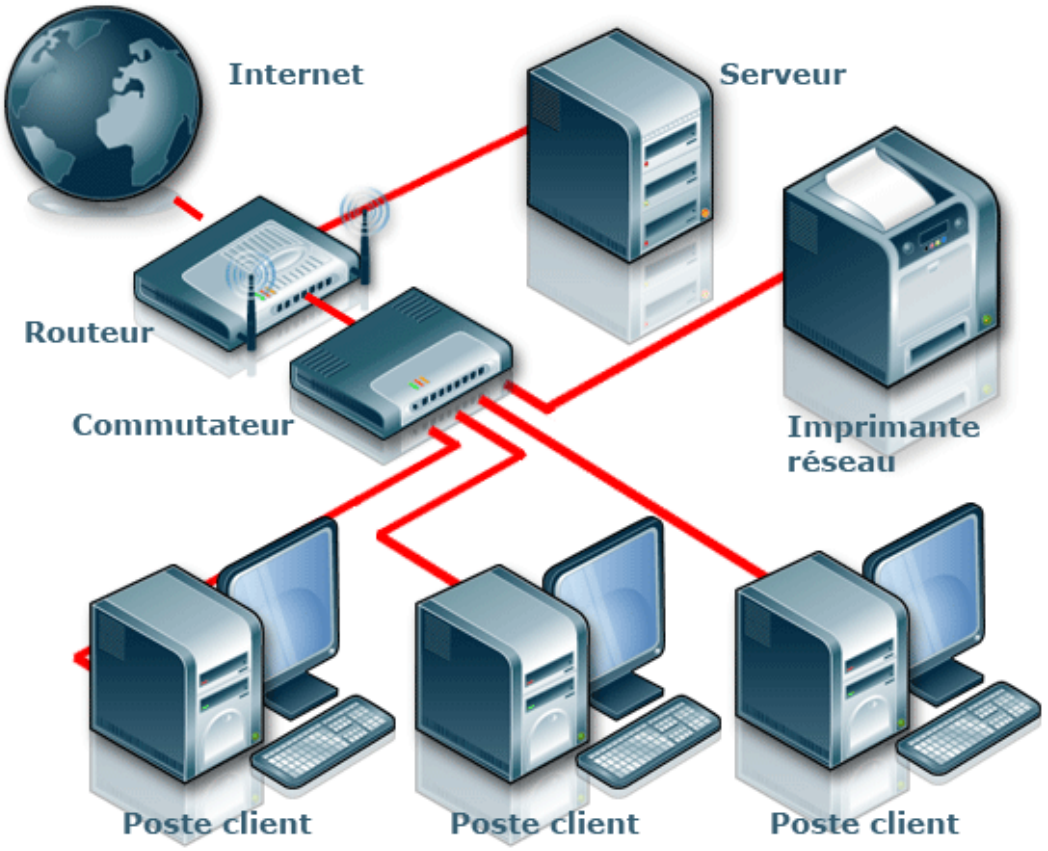
Les PAN (Personal Area Network)

- quelques mètres,
- ils interconnectent les équipements personnels : ordinateur personnel, portables, imprimantes, appareils domestiques, etc.

Réseau personnel (PAN)

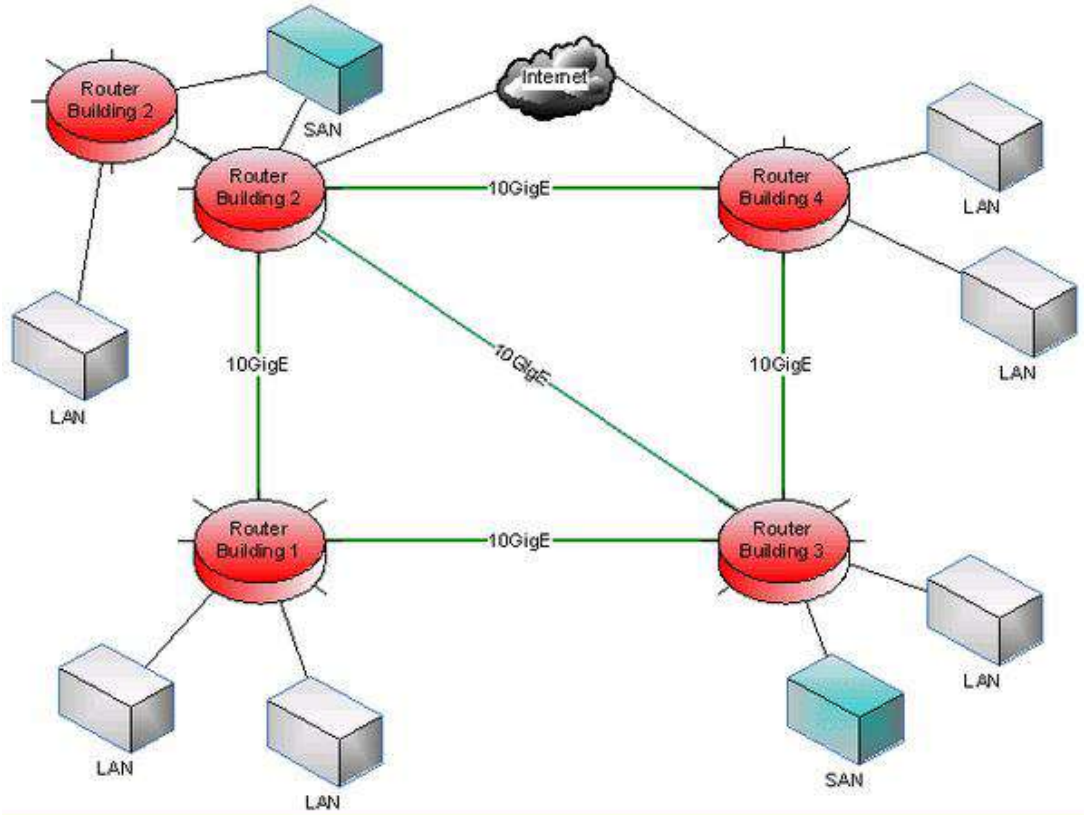
Les réseaux locaux (LAN)

- plusieurs centaines de mètres
- ils interconnectent les équipements informatiques d'une même entreprise, d'une même université
- débit de quelques Mbit/s à quelques Gbit/s
- technologie la plus utilisée : Ethernet



Les réseaux métropolitains (MAN)

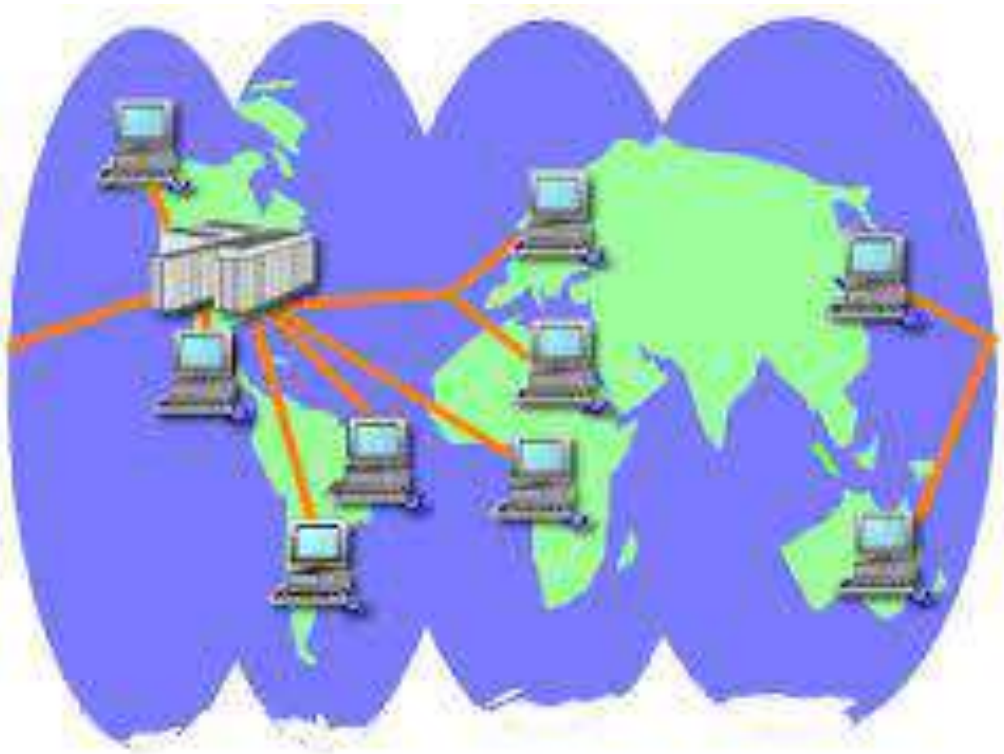
- interconnexion de plusieurs sites dans une même ville
- interconnexion des réseaux locaux situés dans des bâtiments différents.



Réseau métropolitain (MAN)

Les réseaux étendus (WAN)

- constitués d'interconnexions de LAN, voire de MAN, les réseaux étendues sont capables de transmettre des informations sur des milliers de kilomètres à travers le monde entier
- ils sont soit terrestres, soit satellitaires

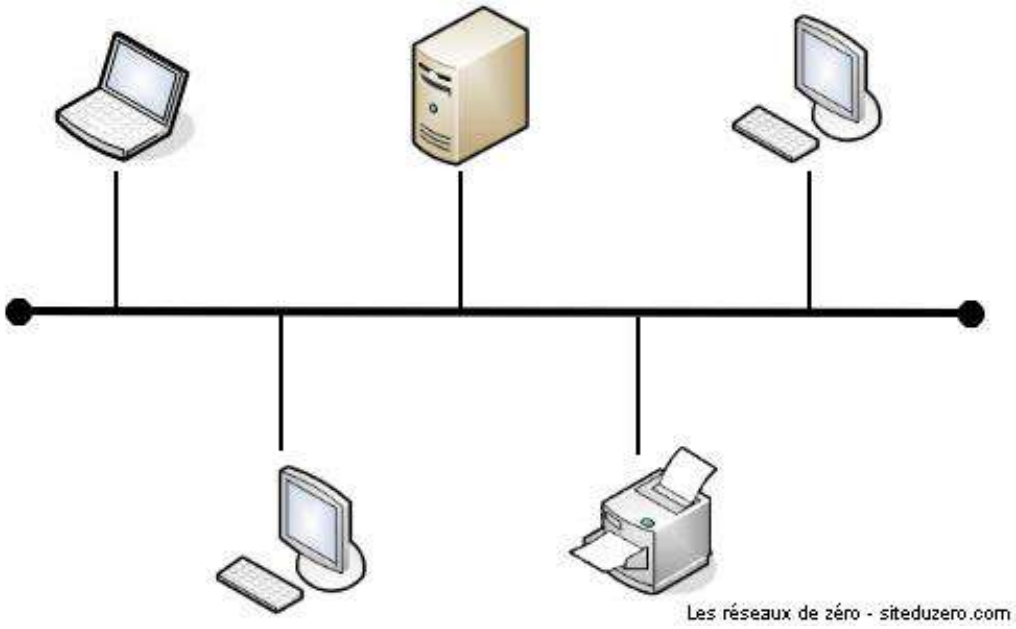


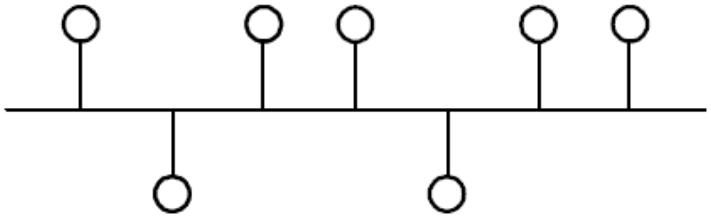
Topologies des réseaux

- La **topologie** du réseau décrit la manière dont les éléments d'un réseau sont disposé les uns par rapport aux autres
- Les topologies les plus utilisées :
  - Bus
  - Anneau
  - Etoile
  - Arbre
  - Maillée

Topologie en bus

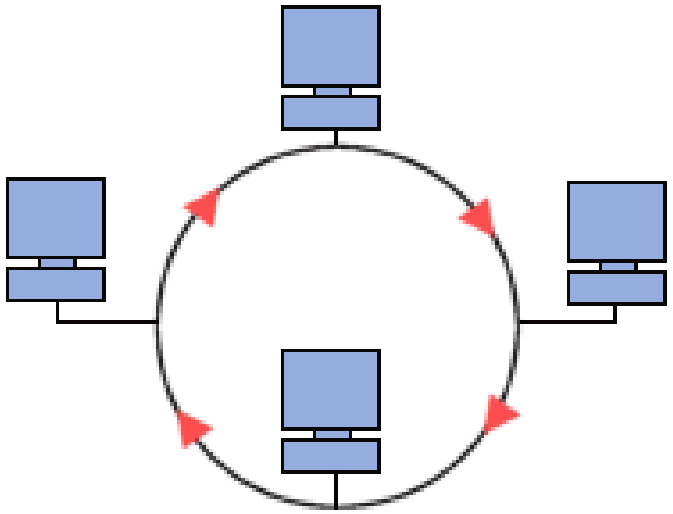
- Le mot «bus» désigne la ligne physique qui relie les machines du réseau





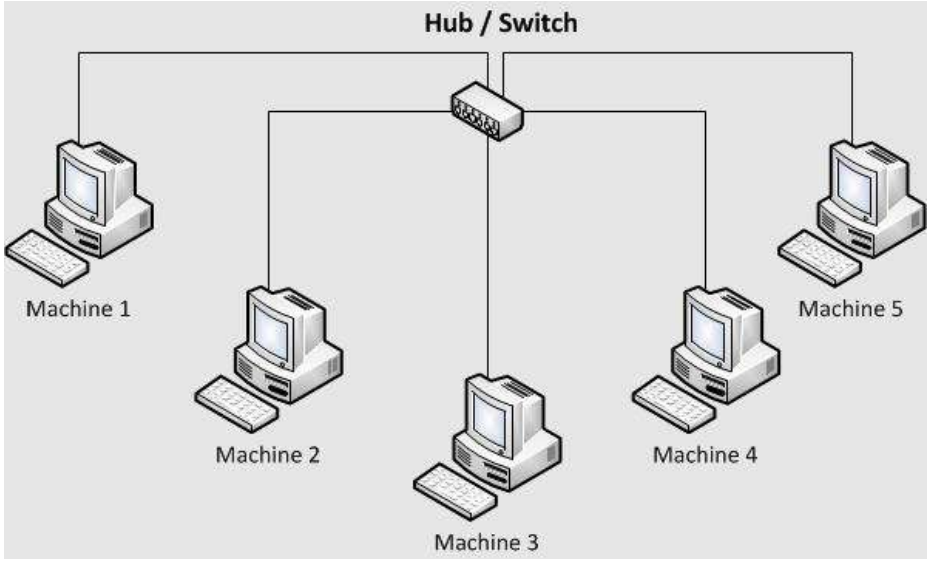
Topologie en anneau

- Les ordinateurs sont situés sur une boucle et communiquent à tour de rôle. Chaque nœud fait office de répétiteur dans la circulation des informations
- Les informations ne circulant dans l'anneau que dans un sens



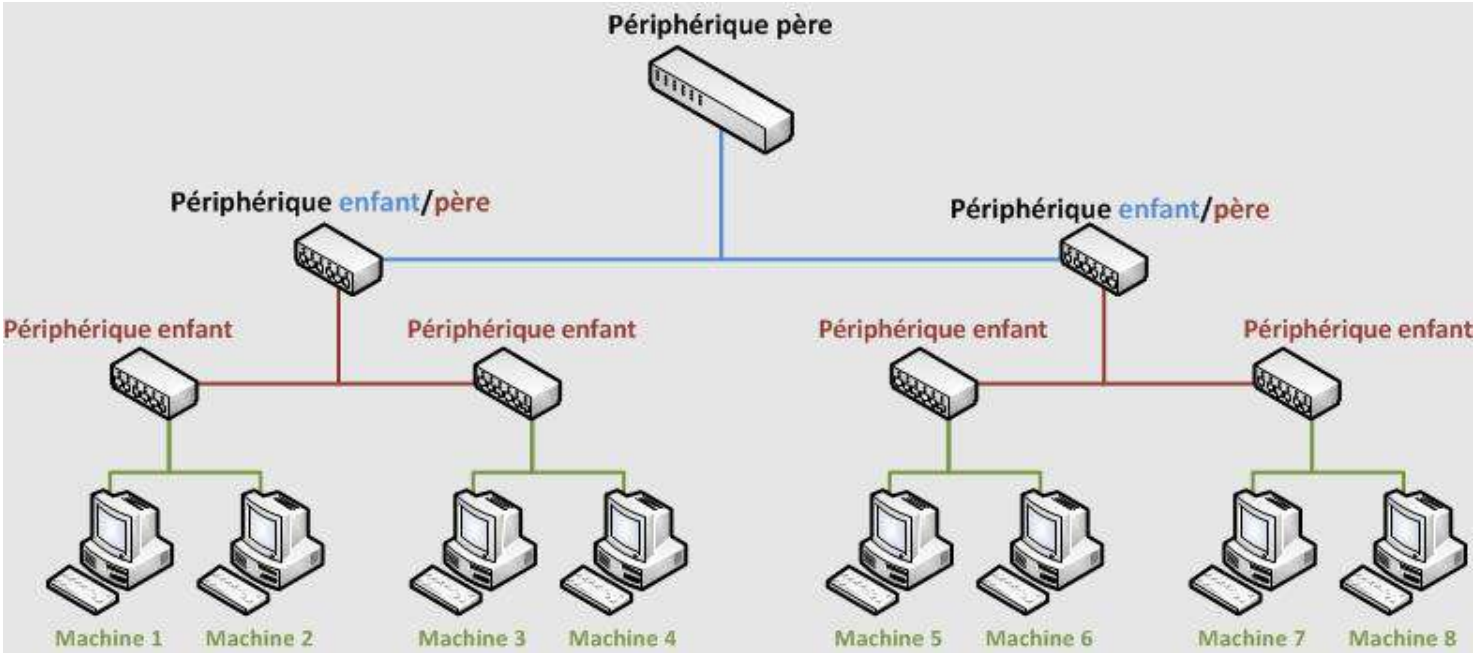
Topologie en étoile

- Les ordinateurs du réseau sont reliés à un nœud central qui est le plus souvent un **concentrateur** ou un **commutateur.** Celui-ci a pour rôle d'assurer la communication entre les différents nœuds
- La plupart des réseaux locaux actuels sont fondés sur cette topologie



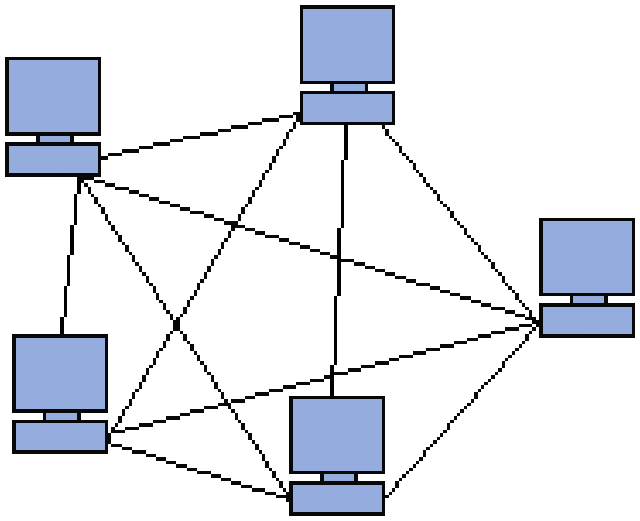
Topologie en arbre

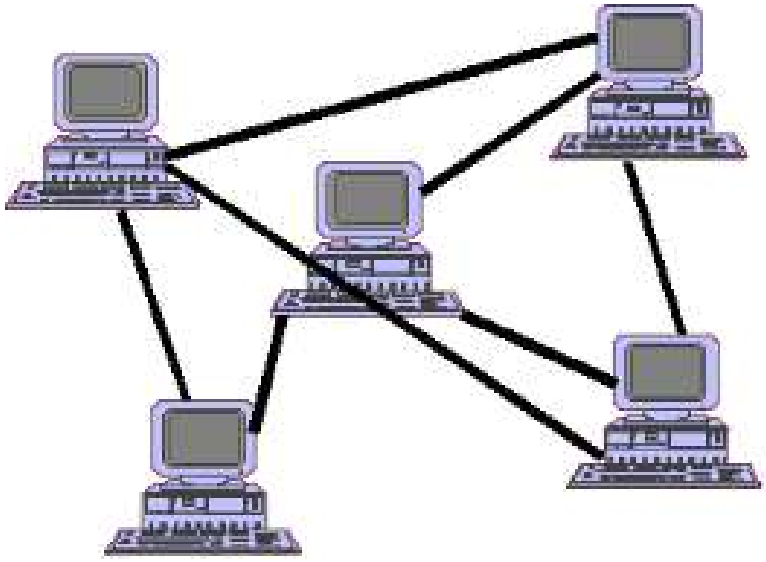
- Cette topologie permet de diviser un réseau en sous-réseaux hiérarchisés



Topologie maillée

- Dans un réseau maillé, chaque nœud est relié à un ou plusieurs autres nœuds sans logique particulière, proposant généralement ainsi plusieurs chemins différents entre deux nœuds quelconques, ce qui renforce la fiabilité du réseau.





Réseaux informatiques

Chapitre 2 – Le modèle OSI

Mustapha Anwar BRAHAMI

ESSA Tlemcen

Références bibliographiques

Ce cours est construit à partir d'un certains nombres de support de cours disponibles sur le net. L'usage de ce composite ne peut être qu'académique :

- DORDOIGNE, J. (2015). *Réseaux informatiques - Notions fondamentales (6ième édition)*. ENI. ISBN : 9782746093928
- LEGRAND, R. (2014). *Notions de base sur les réseaux : 1er module de préparation à la certification CCNA 200-120*. ENI. ISBN : 9782746092136
- DROMARD, D. (2006). *Architecture des réseaux*. Pearson. ISBN : 9782744076640
- LOHIER, S. (2010). *Le réseau Internet : des services aux infrastructures*. Dunod. ISBN : 9782100546046
- PARET, D. (2012). *Réseaux multiplexés pour systèmes embarqués* : CAN, LIN, FlexRay, Safe by Wire. Dunod. ISBN : 9782100582891
- CISCO Systems. *Notions de base sur les réseaux*. CCNA Exploration Fr V 4.0
- FERRAND, P. (2013). *Réseaux*. INSA de Lyon. http://www.ferrand.cc/pdfs/cours_reseaux.pdf
- DUVALLET, C. (2016). *Architecture et protocoles des réseaux*. Université du Havre. http://litis.univ-lehavre.fr/~duvallet/enseignements/Cours/M1INFO/Reseau/MI-Cours-Reseau-Cours1.pdf
- *Réseaux informatiques, modèle OSI, protocole TCP/IP*. http://info.arqendra.net/Files/_Rsx+OSI+TCPIP_cours.pdf
- DE MEY, L. *Structure en couches : Le modèle de référence OSI. www.courstechinfo.be/Reseaux*
- BENNADA, B. (2006). *Réseaux informatiques*. Université de Tlemcen
- FRABOULET, A. (2011). *Introduction aux réseaux*. INSA de Lyon. http://docinsa.insa-lyon.fr/polycop/download.php?id=173834&id2=0
- ABTOY, A., EL KHMLICHI, Y. *Les supports de communications*. École nationale des sciences appliquées de Tétouan

Architecture en couches

- Le concept de couches s'impose en informatique dès qu'il s'agit de subdiviser les tâches d'un système.

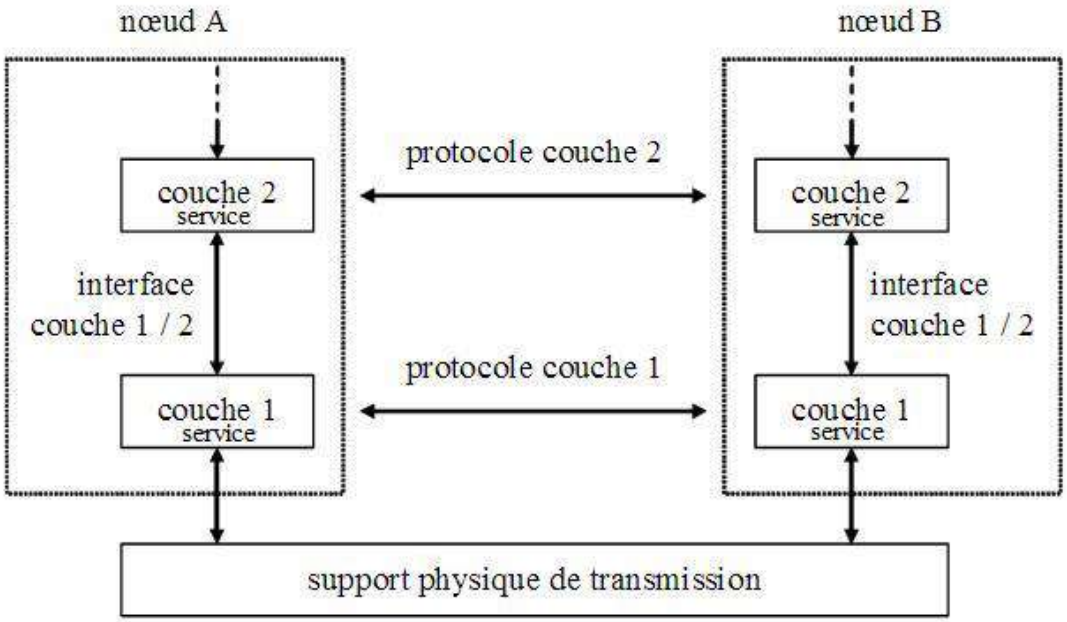
- Il est utilisé au niveau des OS et de plusieurs logiciels.

- On le retrouve au niveau des réseaux.

Architecture en couches

- La plupart des systèmes de télécommunications sont construits selon une architecture en couches → segmentation en plusieurs niveaux, empilés l'un sur l'autre
- Chaque couche réalise une fonction bien déterminée (**service**)
- Chaque couche est liée aux 2 couches adjacentes par la notion d'**interface**, qui est l'ensemble des opérations proposées à la couche supérieure, et utilisées de la couche inférieure
- Deux couches de même niveau de deux nœuds différents peuvent communiquer, en utilisant un **protocole** spécifique

Architectures en couches



Inférieure = plus proche du matériel
Supérieure = plus proche des applications

Chaque couche offre des services à celle qui lui est directement supérieure

Et utilise les services de la couche directement inférieure

La communication entre couches de même niveau est une **communication virtuelle ou logique**

La **communication réelle** (ou physique) se fait entre couches physiques (les plus basses)

Protocole, service et interface

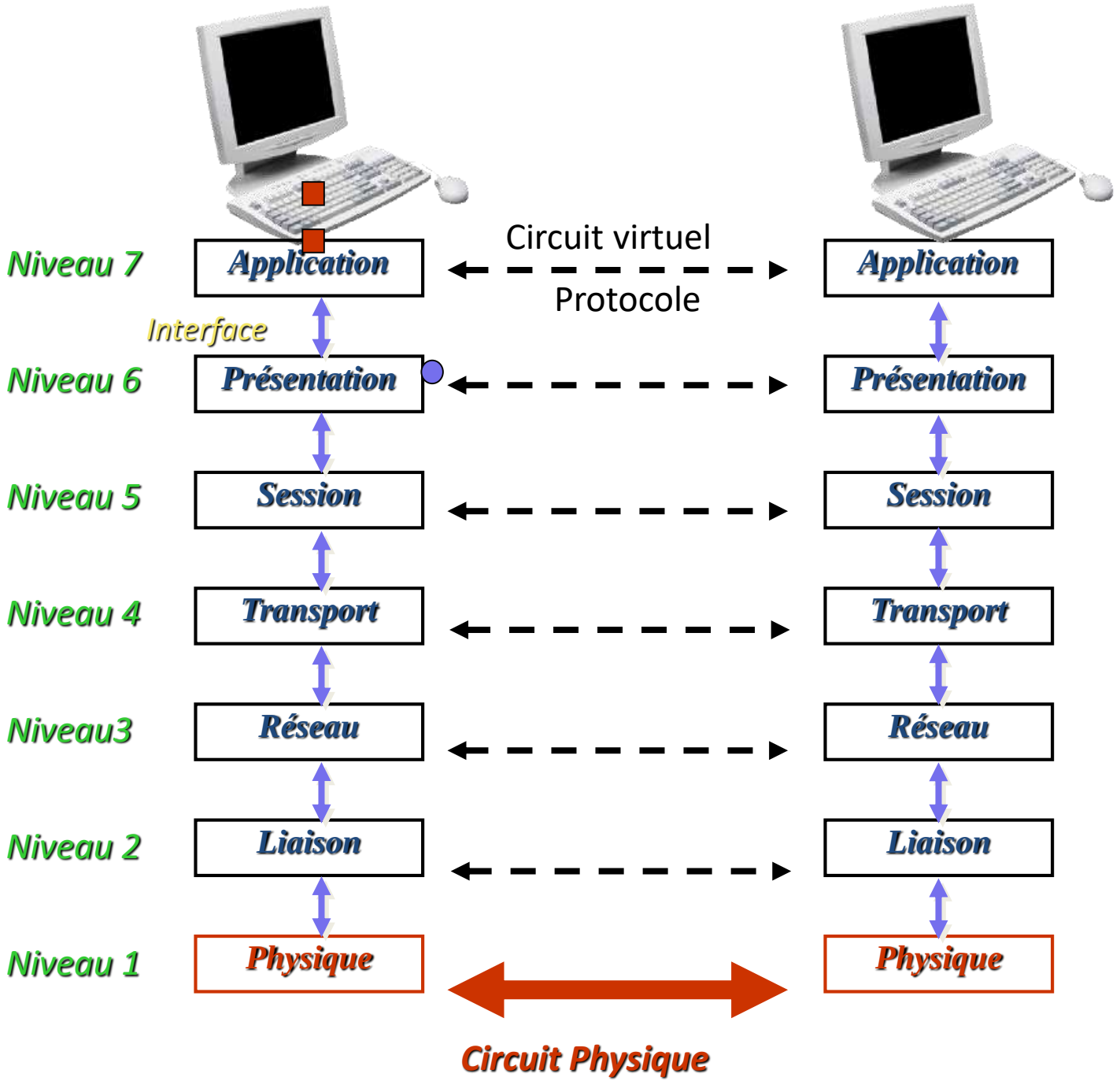
- **Protocole** : un arrangement et des règles, entre les parties communicantes sur la structure des messages échangés ainsi que leurs significations.
- **Service** : implémentation des spécifications imposées par le protocole (fonctions).
- **Interface** : « point d'accès au service », dans un programme, c'est typiquement un ensemble de fonctions de bibliothèque ou d’appels systèmes. Dans une réalisation matérielle, c’est par exemple un jeu de registres à l’entrée d’un circuit.

Avantages des systèmes en couches

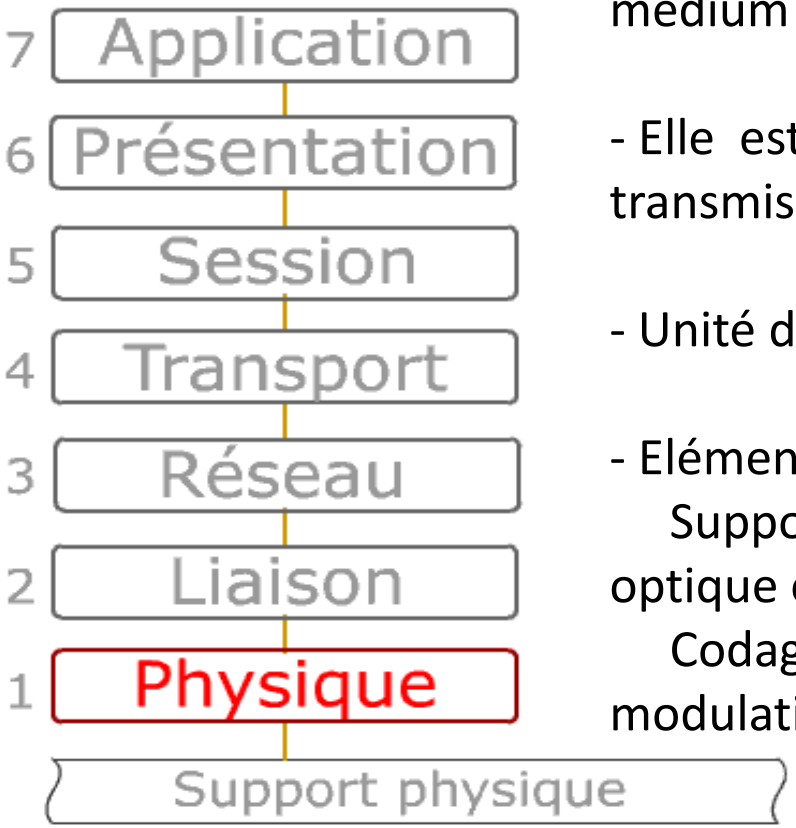
- **Diviser pour mieux régner**; il est plus simple de traiter chaque problème séparément
- Décomposition en modules (couches) relativement simples
- Possibilité de modifier un module sans devoir adapter les autres
- Il est inutile de comprendre tous les détails pour pouvoir comprendre l'ensemble
- Développements, corrections, modifications et évolutions facilitées

Le modèle OSI

- Le modèle OSI (Open Systems Interconnection = Interconnexion de Systèmes Ouverts) est un modèle générique et standard d'architecture d'un réseau en 7 couches, élaboré par l'organisme ISO (International Standardisation Organisation) en 1984.
- Un modèle de référence « papier » et ne correspond pas réellement à une technologie réseau « réelle ».
- Il permet cependant de placer les principes de fonctionnement de manière indépendante d'une implantation.


Niveau 7
Application
Circuit virtuel
Protocole
Application
Interface
Niveau 6
Présentation
Présentation
Niveau 5
Session
Session
Niveau 4
Transport
Transport
Niveau3
Réseau
Réseau
Niveau 2
Liaison
Liaison
Niveau 1
Physique
Physique
Circuit Physique

Couche physique



- Transmettre des séquences de bits via un médium de communication (support physique).

- Elle est en contact direct avec le support de transmission.

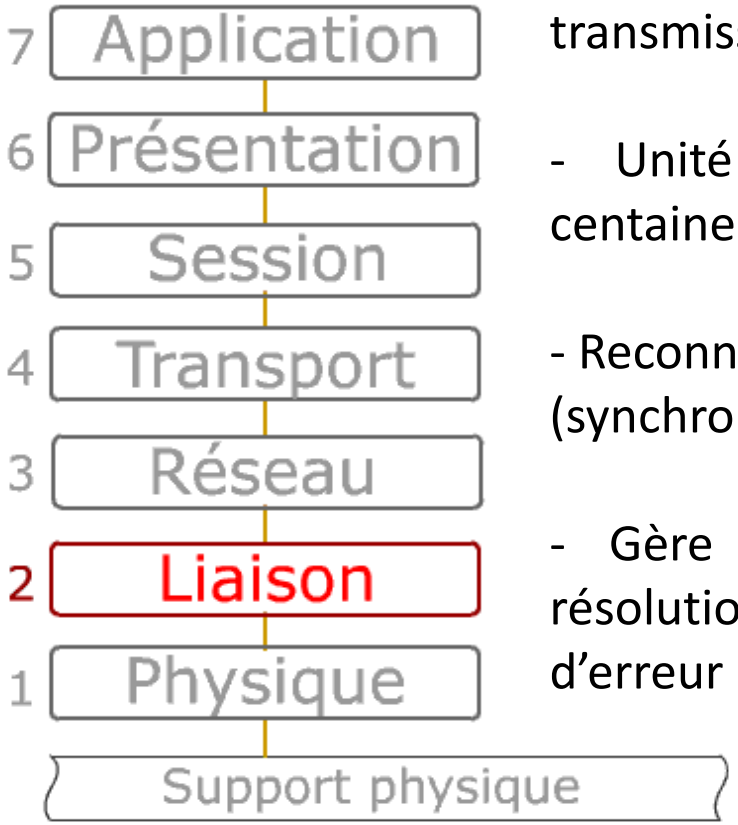
- Unité d'échanges : le bit

- Eléments de la couche physique :

Support physique (paire torsadée, fibre optique etc.)

Codage, modulation (code NRZ, Manchester, modulation AM, FM, etc.)

Couche liaison de données



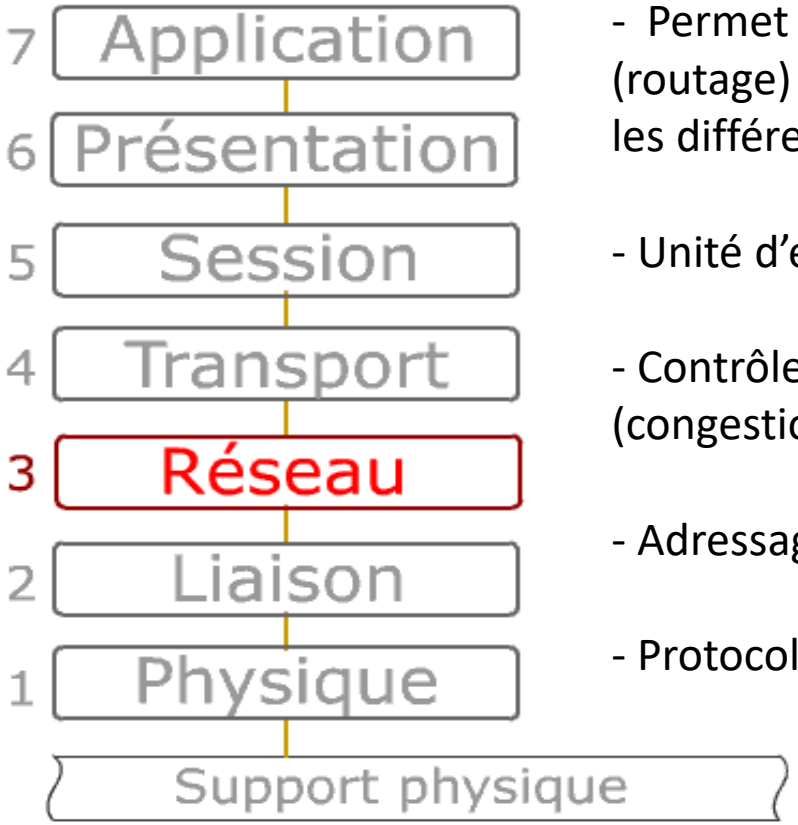
- La couche de liaison des données se charge du formatage des trames et assure leur transmission sans erreurs.

- Unité d'échanges : la trame (quelques centaines ou quelques milliers d'octets).

- Reconnaître les débuts et les fins de trames (synchronisation)

- Gère la méthode d'accès (CSMA …), la résolution d'adressage physique et la détection d'erreur (contrôle de parité, CRC …).

Couche réseau



- Permet de déterminer le choix de la route (routage) entre les nœuds afin de transmettre les différents paquets.

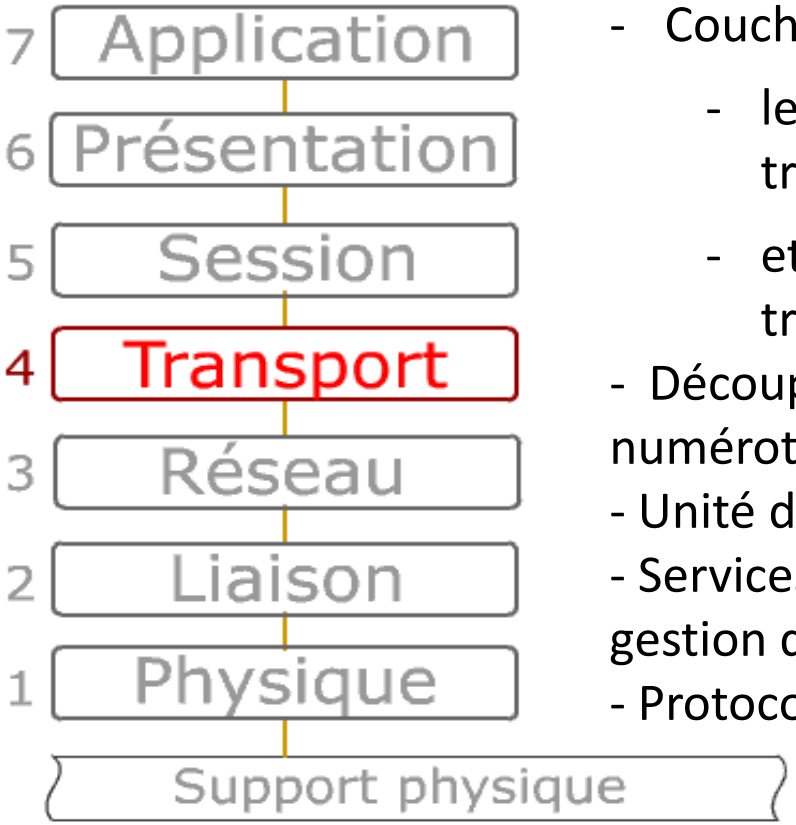
- Unité d'échanges : le paquet.

- Contrôle du flux : éviter les embouteillages (congestion)

- Adressage logique

- Protocoles : IP, X25 …

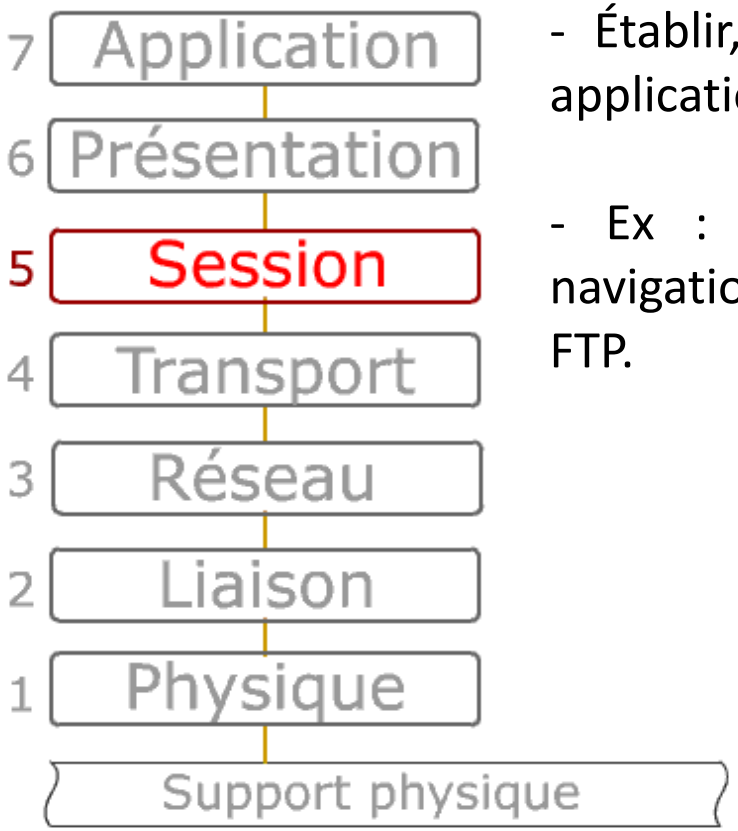
Couche transport



- Couche intermédiaire entre
  - les 3 couches supérieures orientées traitement
  - et les 3 couches inférieures orientées transmission

- Découpe le message en segments qui seront numérotés.
- Unité d'échanges : le segment.
- Services : segmentation, contrôle de séquence, gestion de la qualité de service
- Protocoles : TCP, UDP …

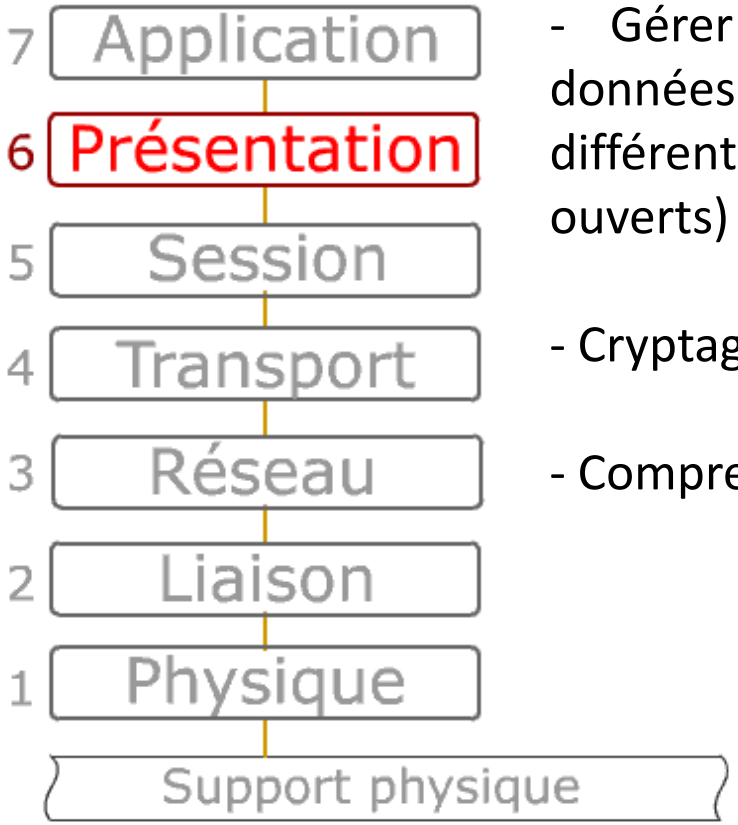
Couche session



- Établir, gérer et terminer les sessions entre applications

- Ex : une connexion HTTP avec suivi de navigation sur un même site web, une connexion FTP.

Couche présentation

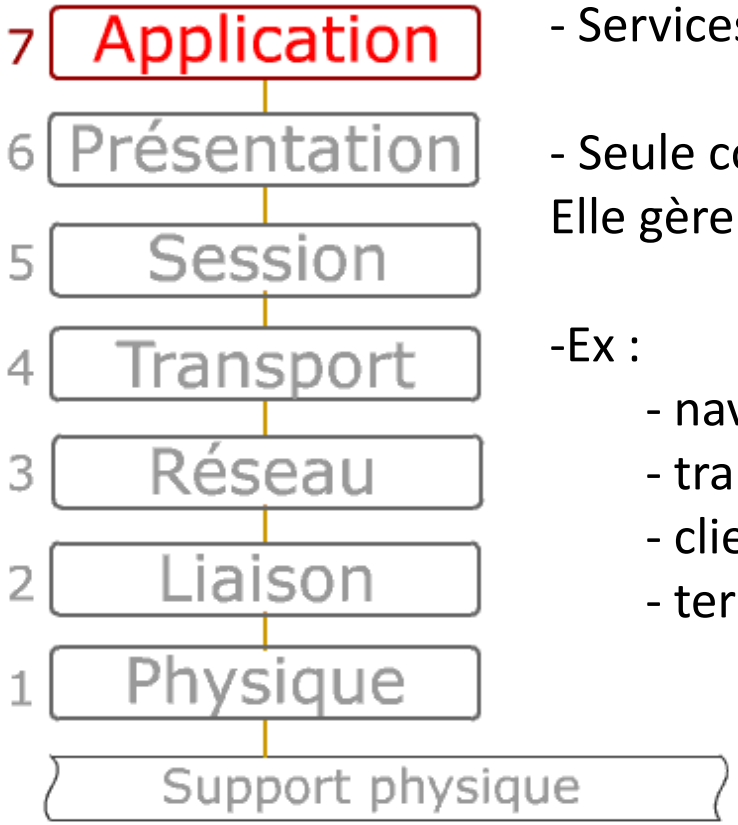


- Gérer la représentation (le codage) des données échangées entre équipements de différente nature (caractéristique des systèmes ouverts)

- Cryptage des données

- Compression des données

Couche application



- Services rendus aux utilisateurs.

- Seule couche en contact avec l'utilisateur
Elle gère son application.

-Ex :
- navigateurs (HTTP),
- transfert de fichiers (FTP),
- clients email (SMTP).
- terminaux virtuels (telnet, ssh...)

Réseaux informatiques

Chapitre 3 – Couche physique

Mustapha Anwar BRAHAMI

ESSA Tlemcen

Références bibliographiques

Ce cours est construit à partir d'un certains nombres de support de cours disponibles sur le net. L'usage de ce composite ne peut être qu'académique :

- DORDOIGNE, J. (2015). *Réseaux informatiques - Notions fondamentales (6ième édition)*. ENI. ISBN : 9782746093928
- LEGRAND, R. (2014). *Notions de base sur les réseaux : 1er module de préparation à la certification CCNA 200-120*. ENI. ISBN : 9782746092136
- DROMARD, D. (2006). *Architecture des réseaux*. Pearson. ISBN : 9782744076640
- LOHIER, S. (2010). *Le réseau Internet : des services aux infrastructures*. Dunod. ISBN : 9782100546046
- FERRAND, P. (2013). *Réseaux*. INSA de Lyon. http://www.ferrand.cc/pdfs/cours_reseaux.pdf
- DUVALLET, C. (2016). *Open System Interconnetion (OSI)*. Université du Havre. http://litis.univ-lehavre.fr/~duvallet/enseignements/Cours/M1INFO/Reseau/MI-Cours-Reseau-Cours2.pdf
- *Réseaux informatiques, modèle OSI, protocole TCP/IP*. http://info.arqendra.net/Files/_Rsx+OSI+TCPIP_cours.pdf
- FRABOULET, A. (2011). *Introduction aux réseaux*. INSA de Lyon. http://docinsa.insa-lyon.fr/polycop/download.php?id=173834&id2=0
- ABTOY, A., EL KHMLICHI, Y. *Les supports de communications*. École nationale des sciences appliquées de Tétouan

Caractéristiques

- Transmission de données binaires au niveau matériel.
- Supports de transmission très variés :
  - câbles électriques, fibres optiques, 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,
- Propriétés des connecteurs et standards 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.

Transmission du signal sur le support

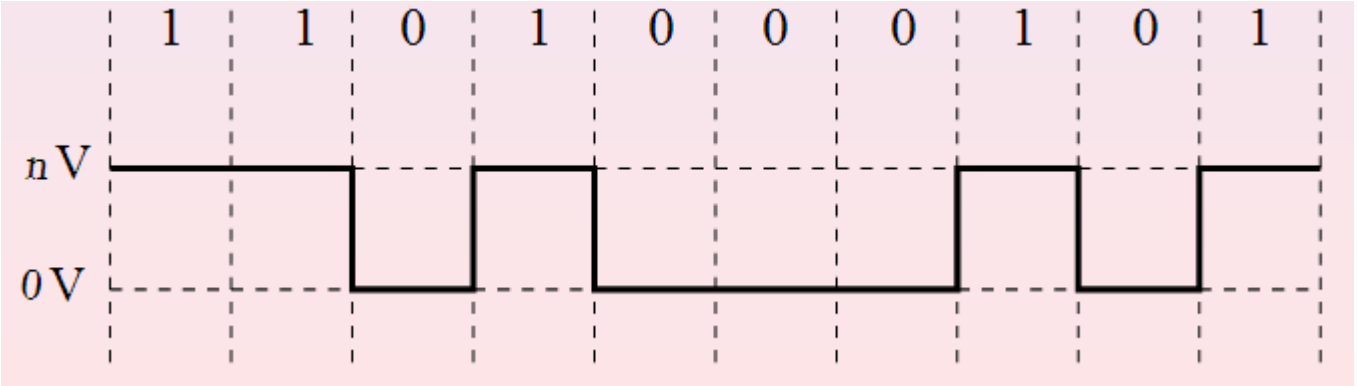
- Quelque soit le support de transmission utilisé, la contrainte reste toujours la même : il faut faire transiter des informations numériques sur un média analogique, de la manière la plus optimale qui soit.
- Il existe deux techniques de transmission :
  - Transmission en bande de base
  - Transmission large bande

Transmission en bande de base

- Les données binaires (signal numérique) sont transmises directement sur le câble : sans modifier la bande de fréquence utilisée (bande de base)
- Utilisée sur des courtes distances (réseaux locaux)
- On fait correspondre 2 niveaux de tension fixes distincts correspondant chacun à un niveau logique (1 ou 0) → Codage

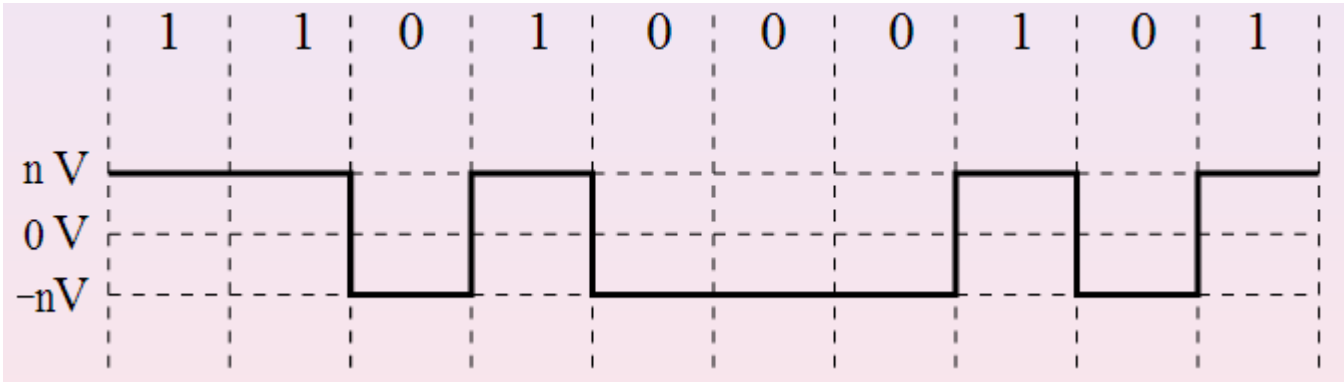
Codage RZ (Return to Zero)

- Codage simple qui consiste à faire correspondre au bit 1 un signal électrique de tension n volts et au bit 0 un signal de tension nulle.
- Problème : une tension nulle correspond à l'envoi d'un 0 binaire mais peut aussi correspondre à l'absence d'envoi de données.



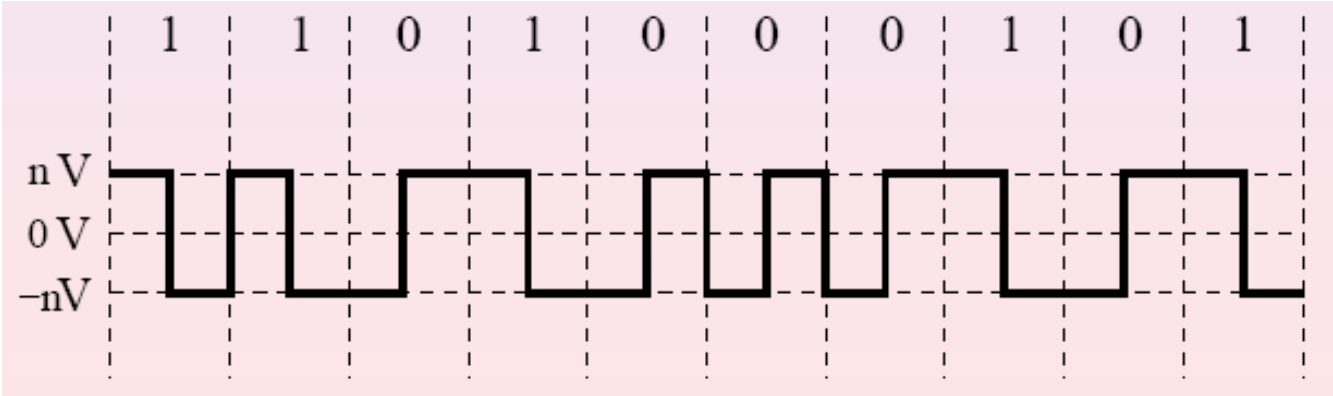
Codage NRZ (No Return to Zero)

- On code le bit 1 par un signal de n volts et le bit 0 par une tension opposée –n volts.
- Résolution du problème d'absence de signal sur le câble.
- Problème : 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.



Codage Manchester

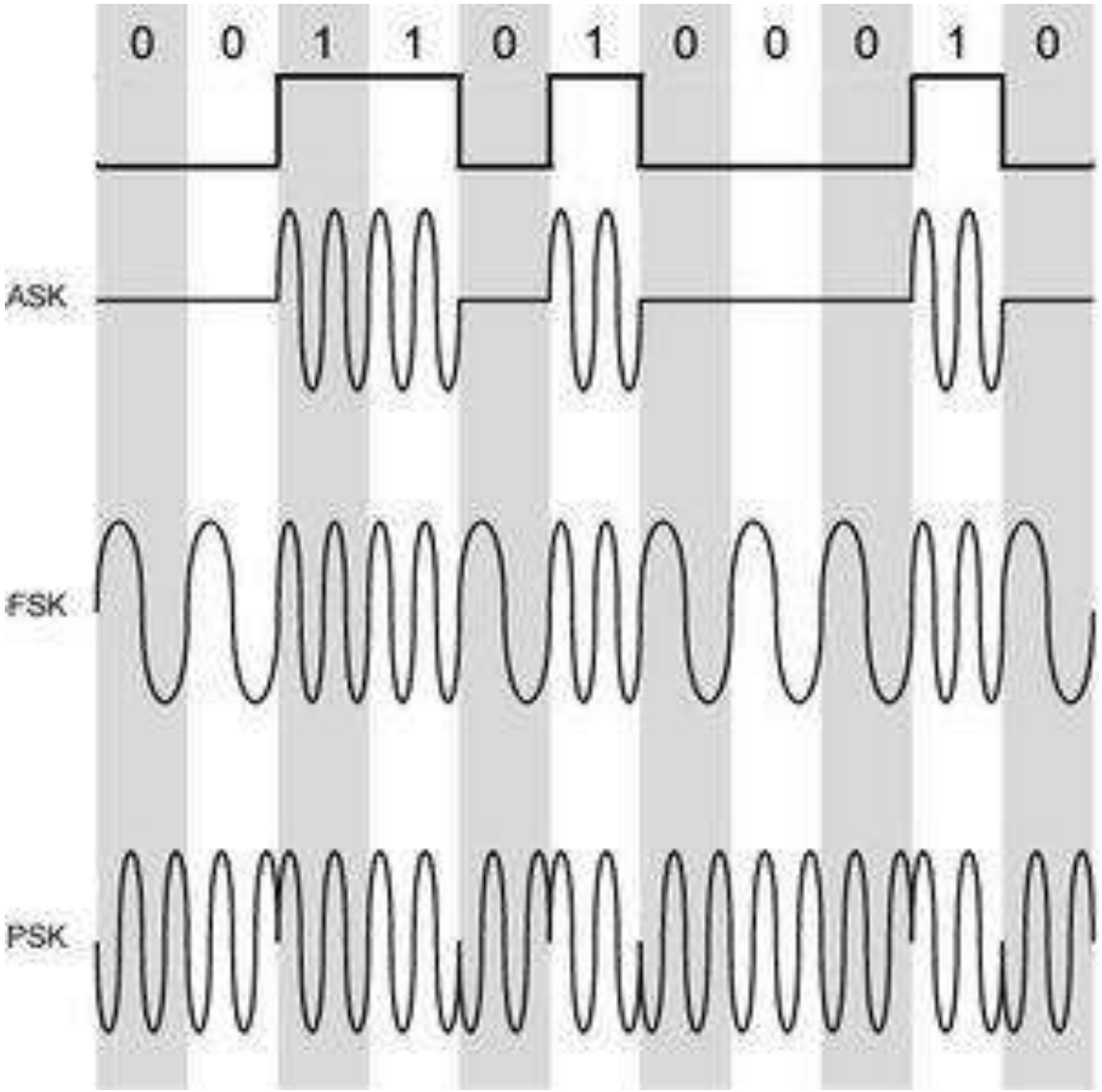
- Il s'agit d'un code basé sur les variations du signal : ce n'est plus la tension qui est importante mais la différence de signal.
- Le bit 1 est codé par un passage de la tension n à -n et le bit 0 par le passage en sens inverse.
- Il propose une solution au problème de détection des longues chaînes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



Transmission large bande

- Transformer le signal numérique en signal analogique par modulation ; on obtient ainsi un seul signal analogique mais porteur d'informations de par la modification de ses caractéristiques dans le temps (fréquence, amplitude, phase).
- Utilisée pour les transmission à haute vitesse sur de longues distances (lignes téléphoniques, faisceaux hertziens, etc.).

Différents types de modulation



Exemples des transmissions

- Liaison série RS-232 : NRZ ;
- USB : NRZI ;
- Ethernet : Manchester ;
- Token Ring : Manchester différentiel ;
- Fibre optique : modulation d’amplitude ;
- Téléphonie, ADSL : modulation de fréquence.

Bande passante et débit

- **Bande passante** : la bande passante représente la quantité d'informations (en bits/s) qui peut être transmise sur un support de transmission (quantité maximale possible).
- **Débit** : le débit est la quantité de données qui transite sur un réseau pendant une durée déterminée (quantité réelle).

Unité de bande passante	Abréviation	Équivalence
Bits par seconde	bits/s	unité de bande passante fondamentale
Kilobits par seconde	Kbits/s	1 kbit/s = 1000 bits/s = 10^3 bits/s
Mégabits par seconde	Mbits/s	1 Mbit/s = 1 000 000 bits/s = 10^6 bits/s
Gigabits par seconde	Gbits/s	1 Gbit/s = 1 000 000 000 bits/s = 10^9 bits/s
Térabits par seconde	Tbits/s	1 Tbits/s = 1 000 000 000 000 bits/s = 10^{12} bits/s

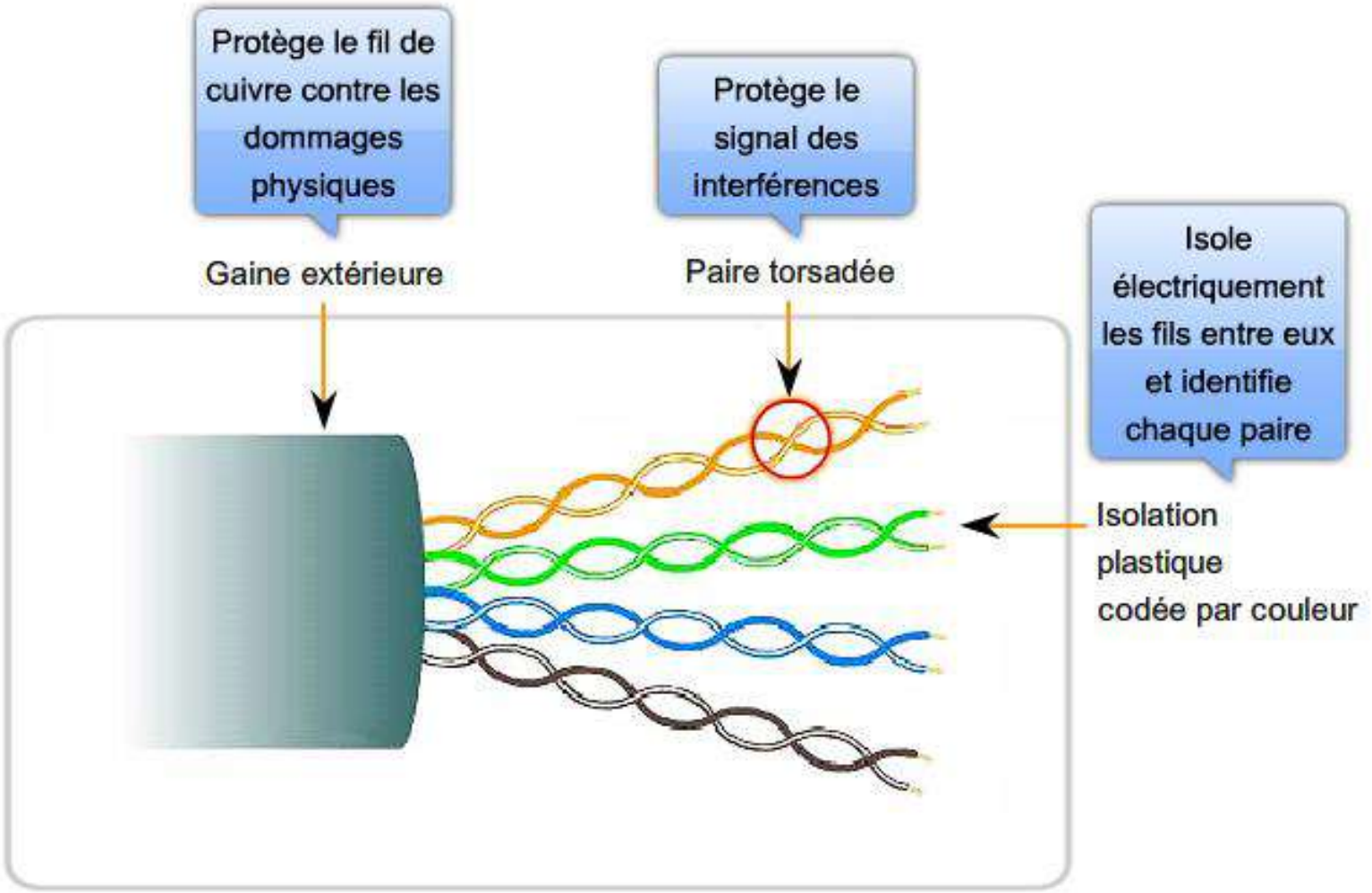
Supports de transmission

- Il existe différents supports de transmission des données. En réseau informatique, on distingue plusieurs sortes de support de transmission:
  - les supports en cuivre: câbles à paires torsadées et câbles coaxiaux,
  - la fibre optique,
  - l'espace hertzien pour les réseaux sans fil.

Câbles à paires torsadées

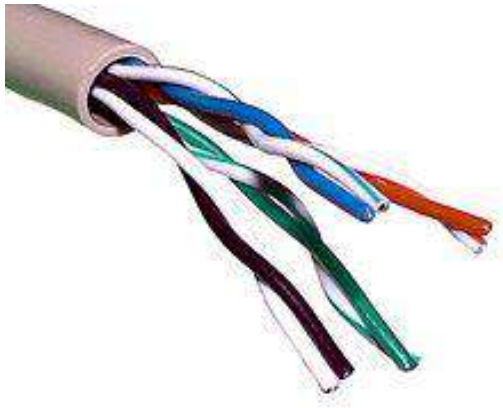
- Il est actuellement le support physique le plus utilisé.
- Il est utilisé dans plusieurs cas :
  - connexion d'un poste au concentrateur du réseau (hub, switch,...).
  - interconnexion d'éléments actifs de natures diverses (concentrateurs, commutateurs, relanceurs...).
- La structure de ce type de câbles est simple : il est constitué de plusieurs fils de cuivre torsadés par paires (pour diminuer la diaphonie).
- Généralement, constitué de quatre paires torsadées (réseaux informatiques) et de deux paires pour le câble téléphonique

Câbles à paires torsadées



Types de paires torsadées

- Pour limiter les interférences, les paires torsadées sont souvent blindées. Le type de câble dépend du blindage utilisé:
  1- le câble non blindé, UTP (Unshielded Twisted Pair), support le plus simple et donc le moins coûteux.
  2- le câble avec écran, FTP (Foiled Twisted Pairs). L'écran est une simple feuille d'aluminium placée entre les fils et la gaine PVC.

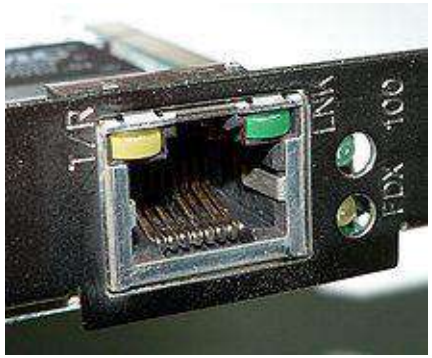


Types de paires torsadées

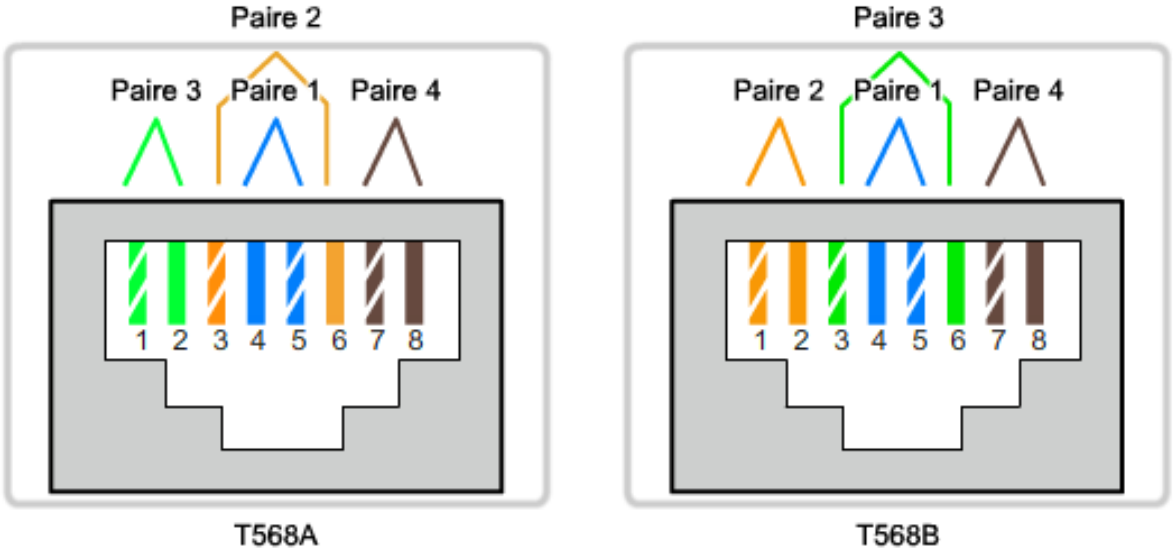
3- le câble blindé, STP (Shielded Twisted Pair), chaque paire est protégée des parasites par un blindage (écran en aluminium ou tresse métallique).

Connecteurs et normes de câblage

- Connecteur : terminaison du câblage → RJ45 (8 broches).



- Deux normes principales de câblage :
  - T568A
  - T568B



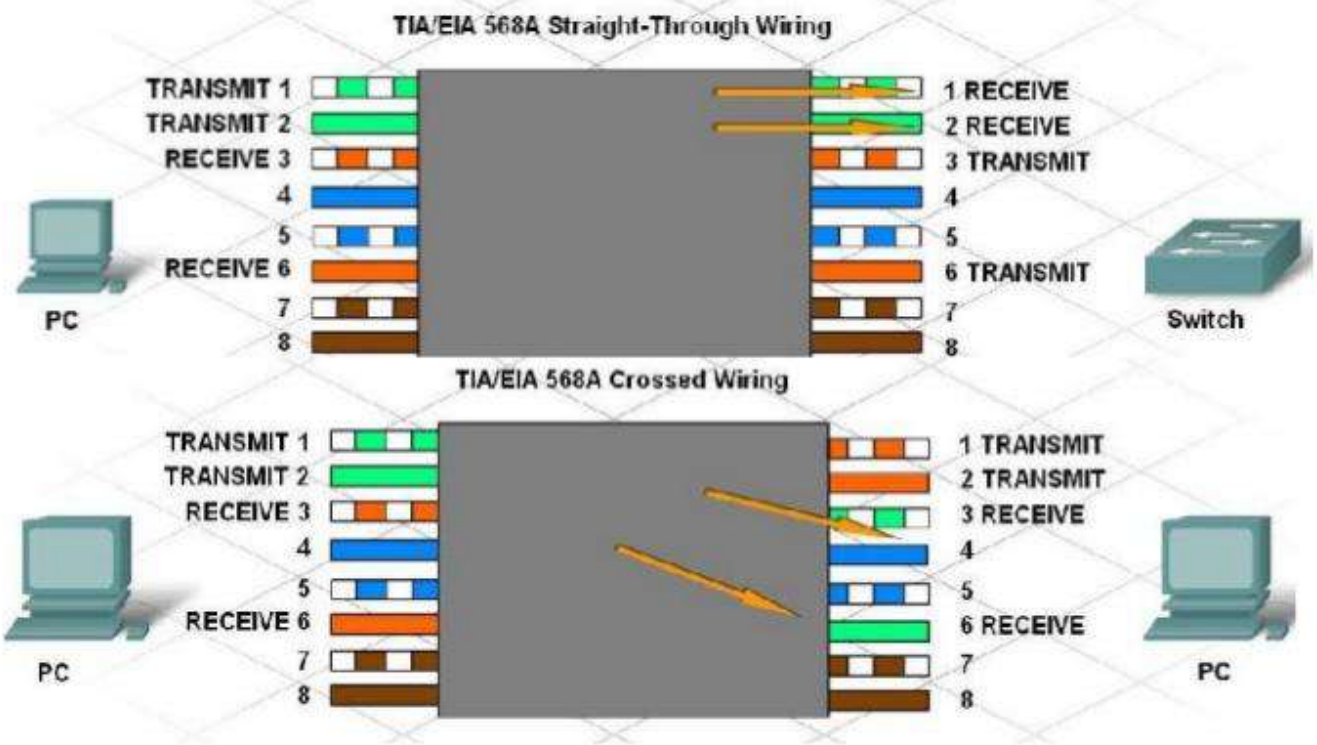
Câbles droits et câbles croisés

- Les commutateurs (switchs) et concentrateurs (hubs) sont identifiés comme étant des DCE (Data Connexion Equipement) alors que les stations terminales et les routeurs sont des périphériques DTE (Data Terminal Equipment). **Les équipements identiques DTE/DTE ou DCE/DCE se connectent avec un câble croisé** (qui croise les paires d'émission et de réception). **Les équipements de type différents se connectent avec un câble droit** car la position émission réception sur leur interfaces est déjà inversée.
- Les nouvelles gammes de matériel réseau s'adaptent automatiquement aux câbles en reconnaissant les positions du signal (émission et réception).

Câbles droits et câbles croisés

Utilisation du câblage à paires torsadées

- Code de couleur : Câble droit, Câble croisé

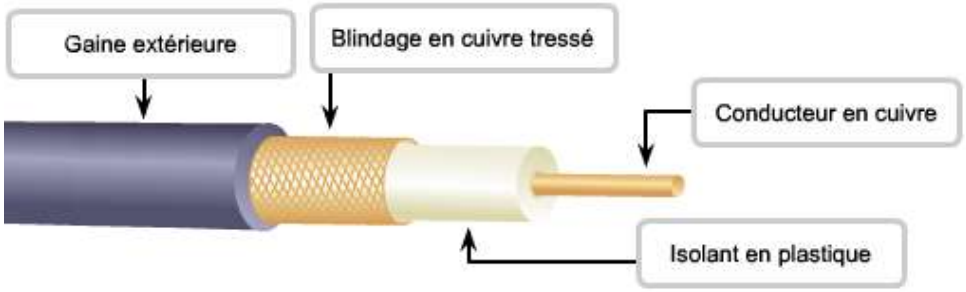


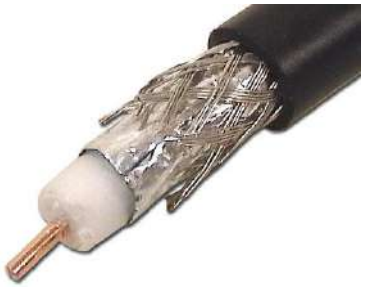
Câbles à paires torsadées

- Avantages:
  - Faible coût.
  - Flexible.
- Inconvénients:
  - Courtes distances (maximum 100 mètres).
  - Vulnérable aux interférences.

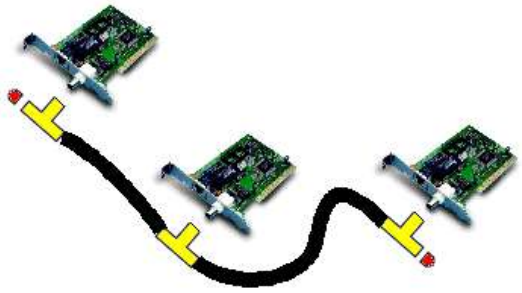
Câble coaxial

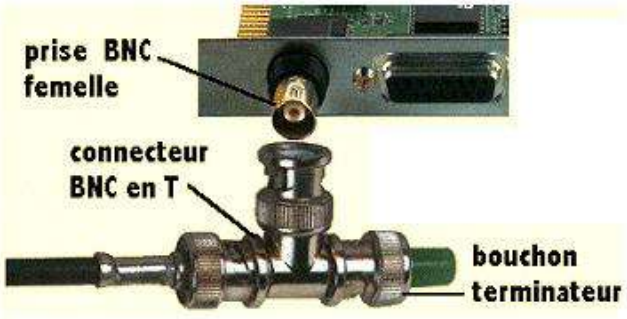
- Se compose d'un conducteur de cuivre entouré d'une couche de matériau isolant flexible.





- Utilisé dans les topologies en bus.
- Connecteur : BNC (British Naval Connector).





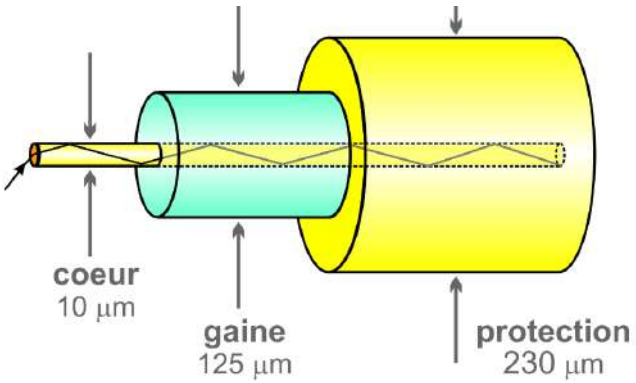
Câble coaxial

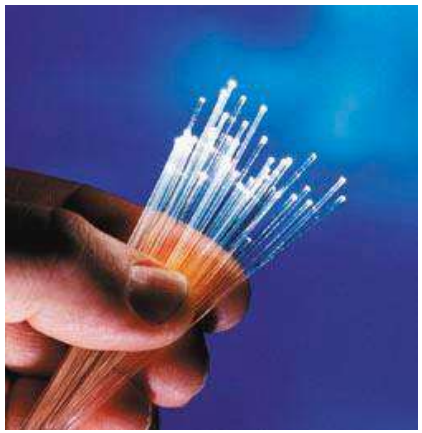
- Avantages:
  - La distance maximale peut atteindre 500 mètres.
  - Bonne résistance au bruit.

- Inconvénients:
  - La rigidité (moins flexible).
  - Support qui tend à disparaître (dans les réseaux informatiques).

La fibre optique

- Une fibre optique est un fil en verre ou en plastique très fin qui a la propriété de conduire la lumière.
- La fibre permet la transmission de données à haut débit grâce à des rayons optiques.
- Connexion à la fibre effectuée par un émetteur optique qui convertit un signal électrique en un signal lumineux.
- Utilisation intéressante même dans des réseaux bas débit pour réduire le taux d'erreurs de transmissions et le nombre de retransmissions.

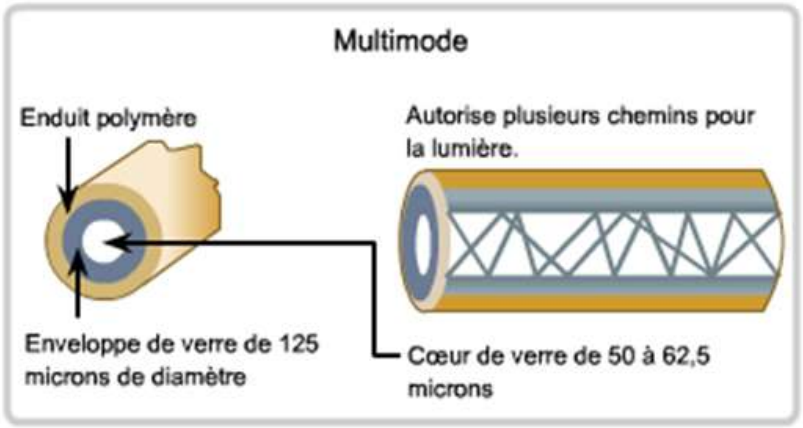




La fibre optique

1 – Fibres multimodes:

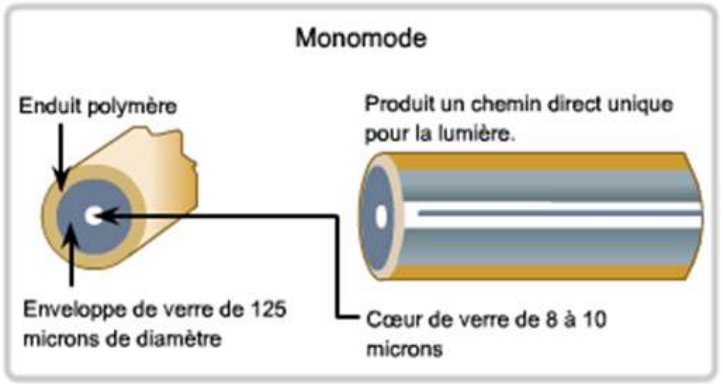
- Le rayon lumineux est transmis par réfractions successives.
- Des performances d'environ 1 Gbit/s sur un kilomètre au maximum.
- Adapté aux réseaux locaux hauts débits.
- Le câble le moins cher pour les fibres optiques.



La fibre optique

2- 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 sur des longues distances (réseaux étendus).
- Un coût de mise en œuvre très élevé notamment à cause des faisceaux lasers.



La fibre optique

- Permet des communications bidirectionnelles simultanées avec un câble dédié à chaque direction.

- Connecteurs:
  - SC: un ergot maintient le connecteur en place une fois enclenché.
  - ST: le branchement est réalisé par un système à baïonnette.

La fibre optique

- Avantages:
  - Débit.
  - Légèreté.
  - Immunité au bruit.
  - Faible atténuation.

- Inconvénients:
  - Coût plus élevé.

Les réseaux sans fils

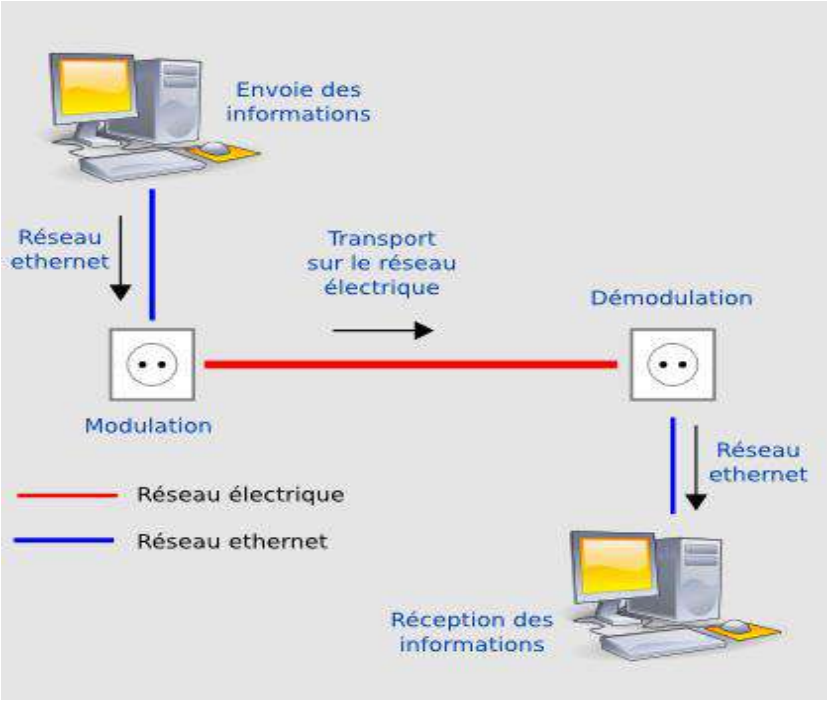
- Utilisation de milieux comme l'air, le vide... comme support de transmission des ondes électromagnétiques : l'espace hertzien.
- Plusieurs types d'ondes électromagnétiques sont utilisées :

Les réseaux sans fils

- Avantages:
  - Mobilité.
  - Facilité de déploiement.
- Inconvénients:
  - Sécurité (média partagé).
  - Sensibilité aux interférences.

Autres supports

- Le transfert d'informations numériques en passant par les lignes électriques:
  - **CPL** : **C**ourants **P**orteurs en **L**igne.



Réseaux informatiques

Chapitre 4 – Liaison de données

Mustapha Anwar BRAHAMI

ESSA Tlemcen

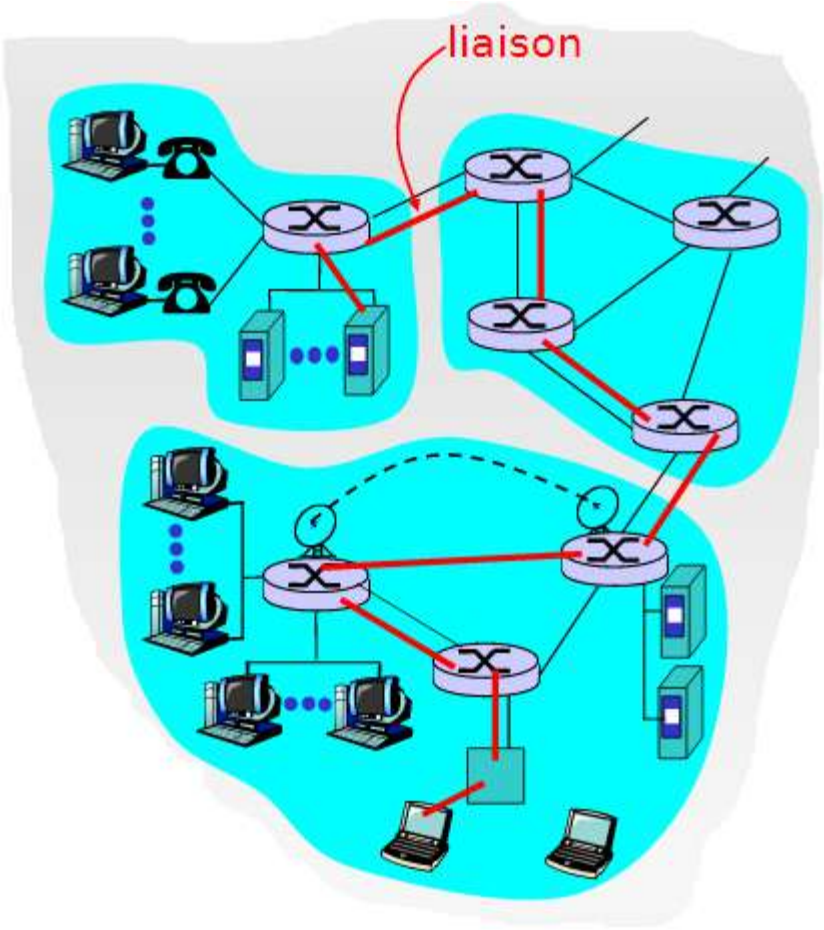
Références bibliographiques

Ce cours est construit à partir d'un certains nombres de support de cours disponibles sur le net. L'usage de ce composite ne peut être qu'académique :

- DORDOIGNE, J. (2015). *Réseaux informatiques - Notions fondamentales (6ième édition)*. ENI. ISBN : 9782746093928
- LEGRAND, R. (2014). *Notions de base sur les réseaux : 1er module de préparation à la certification CCNA 200-120*. ENI. ISBN : 9782746092136
- DROMARD, D. (2006). *Architecture des réseaux*. Pearson. ISBN : 9782744076640
- LOHIER, S. (2010). *Le réseau Internet : des services aux infrastructures*. Dunod. ISBN : 9782100546046
- FERRAND, P. (2013). *Réseaux*. INSA de Lyon. http://www.ferrand.cc/pdfs/cours_reseaux.pdf
- DUVALLET, C. (2016). *Open System Interconnetion (OSI)*. Université duHavre.http://litis.univlehavre.fr/~duvallet/enseignements/Cours/M1INFO/Reseau/MI-Cours-Reseau-Cours2.pdf
- Cours couche liaison de données. ENS Kouba.

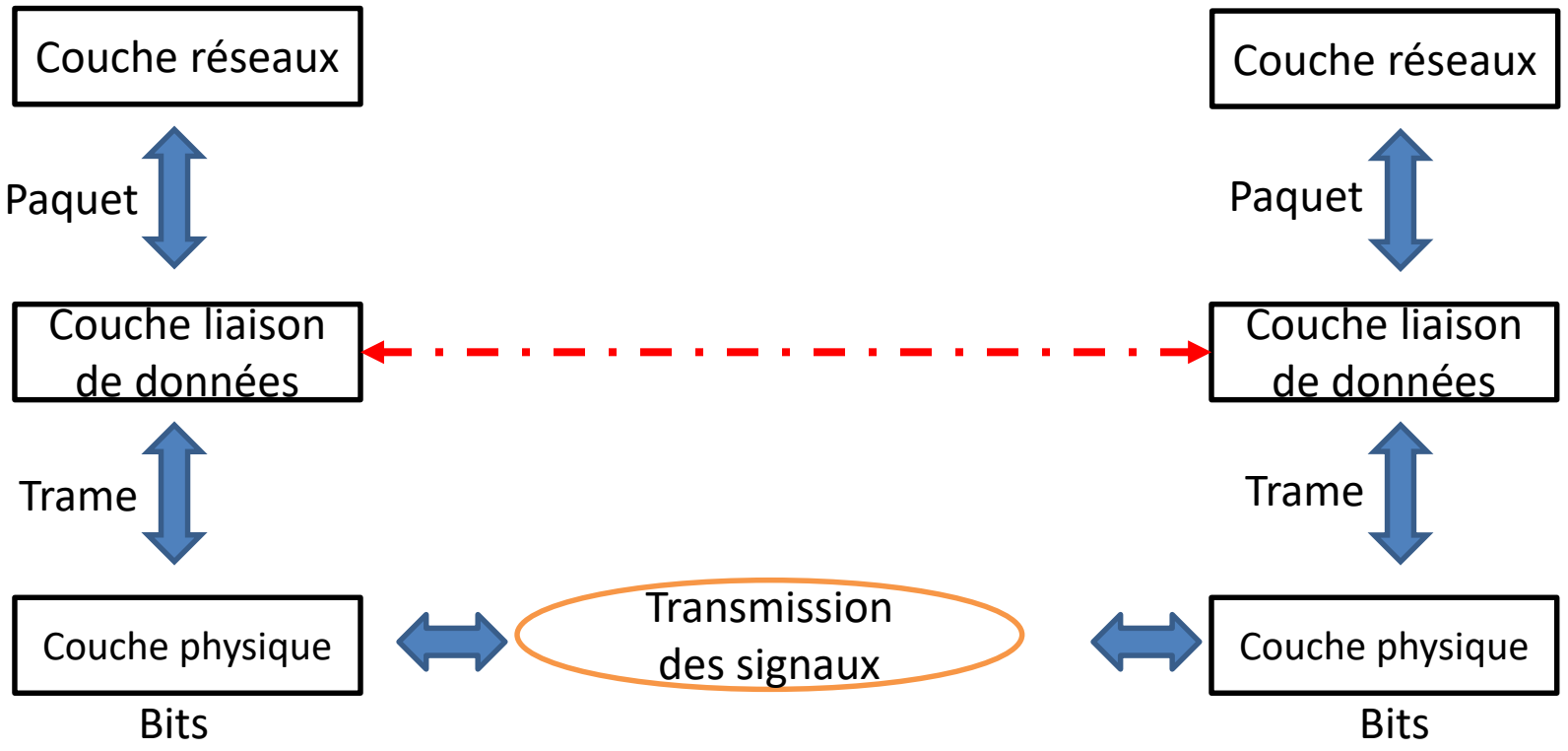
Liaison de données

- La couche liaison a la responsabilité de transférer des données d'un nœud à un nœud adjacent sur une liaison.



Liaison de données

- L'unité d'information associée à la couche 2 du modèle OSI est la **trame** ou L-PDU.

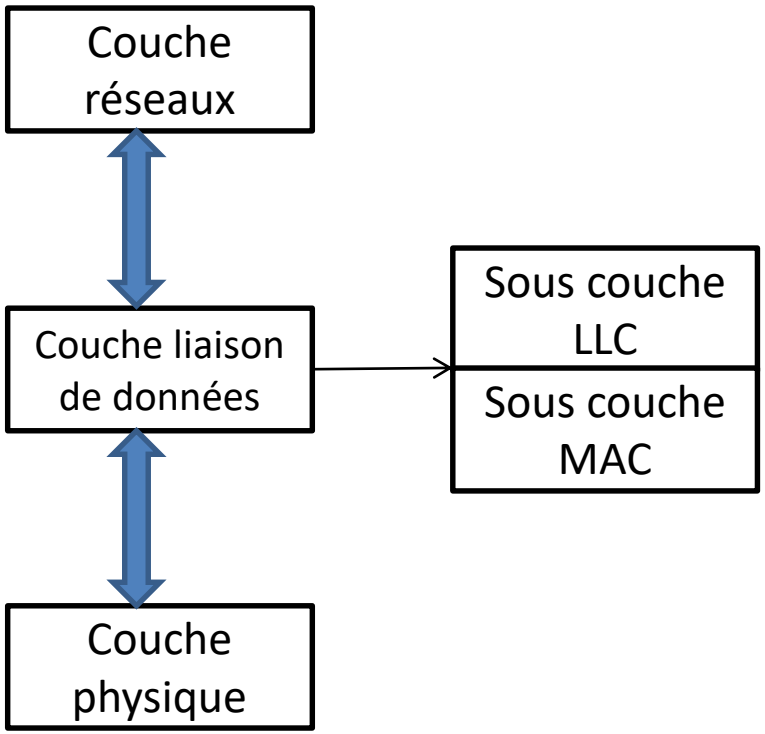


Services de la couche Liaison de données

- Utiliser les services fournis par la couche physique.
- Fournir plusieurs services :
  - Découpage en trame : délimiter les données issus de la couche réseau.
  - Contrôle d'accès au media de transmission : quelle machine a le droit d'utiliser le support pour envoyer les données.
  - Adressage : identification physique des machines.
  - Contrôle d'erreurs : assurer le transfert sans erreurs des données.
  - Contrôle de flux : assurer un transfert fiable de données.

Sous-couches de la couche liaison de données

- La couche liaison de données est découpée en deux sous-couches :
  - La sous-couche MAC (Media Access Control).
  - La sous-couche LLC (Logical Link Control).



Sous-couche MAC

- La sous couche MAC (Media Access Control) a pour rôle de :
  - structurer les bits d'information en trames (tramage).
  - gérer l'accès au support physique.
  - gérer les adresses physiques des interfaces de communication.
- Elle est indépendante du média : câble cuivre, fibre optique, onde hertzienne …

Sous-couche LLC

- La sous-couche LLC (Logical Link Control) est l'interface avec la couche Réseau. Elle a pour rôle :
  - La protection contre les erreurs de transmission.
  - Assurer le transfert des trames et le contrôle de flux entre les stations du réseau.

Sous-couche MAC

Notion de trame

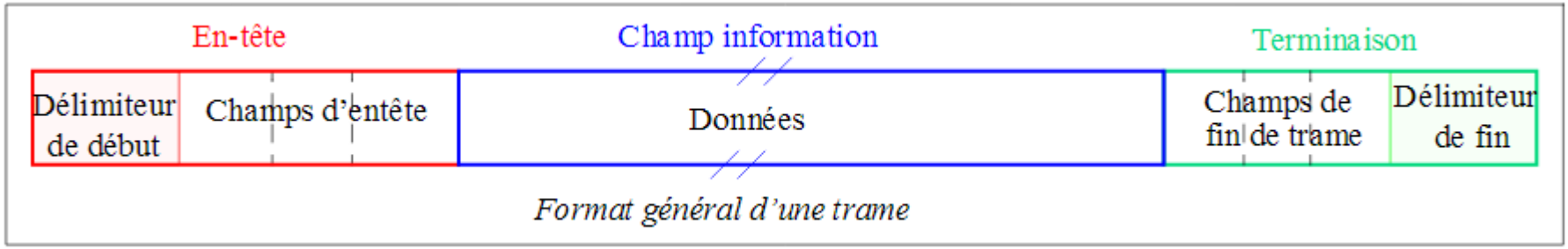
- C’est l’unité de données de la couche Liaison de données.
- Comporte des champs de différentes tailles :
  - les champs de contrôle (en nombre fixe ou variable).
  - le champ de données.
  - le protocole utilisé permet de reconnaître tous les champs.

Notion de trame

- Suivant le type de protocoles, une trame peut :
- (i) être de taille fixe ou de taille variable (jusqu'à une certaine taille maximum).
  - Exemple :
    - variable = trame d'HDLC,
    - fixe = cellule d'ATM (53 octets)
- (ii) ne pas avoir de fin de trame explicite.
  - Exemple :
    - SD + ED (''Starting/ending delimiter'') = trame d'HDLC ou Token Ring,
    - SD uniquement : trame Ethernet

Format général d'une trame

- Le début et la fin de trame sont souvent identifiés par des délimiteurs.
- Composée d'un certain nombre de champs ayant chacun une signification précise.
- On distingue souvent 3 ensembles de champs : l'entête (« header »), le champ de données et la terminaison (« trailer »).



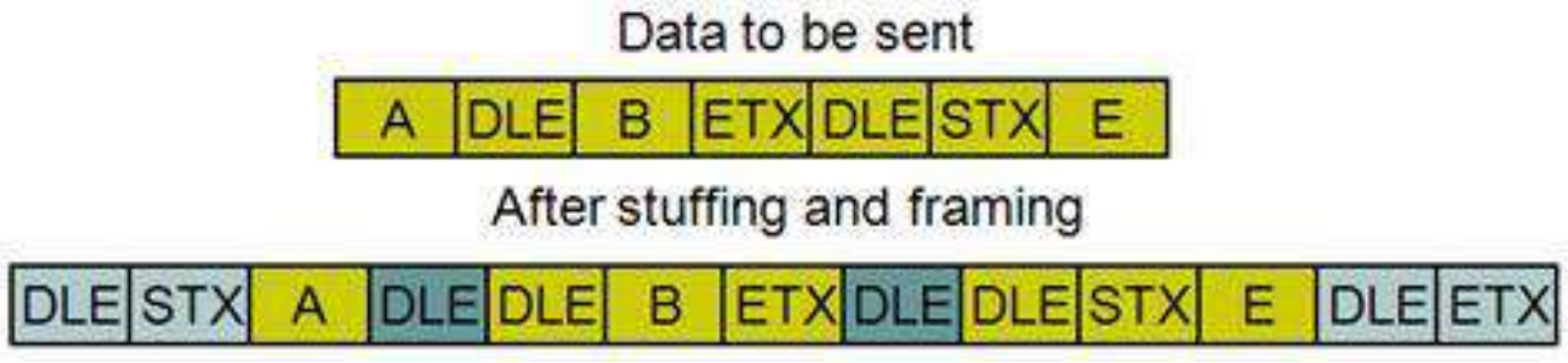
Format général d'une trame

Délimiteurs et synchronisation

- Plusieurs techniques possibles :
  - Caractères spéciaux (protocole BSC d'IBM)
  - Fanions (protocole HDLC)
  - Violation du codage (protocole Ethernet)

Délimiteurs et synchronisation : caractères spéciaux

- 3 caractères sont pris sur le jeu de caractères : DLE, STX et ETX
- le début est marqué par la séquence DLE STX
- la fin par DLE ETX
- DLE est utilisé pour la transparence : ajouté devant chaque DLE des données.



Délimiteurs et synchronisation : fanions

- une séquence de bits (fanion) est le délimiteur.
- généralement 01111110
- un bit à 0 est ajouté après toute suite de 5 bits à 1 dans les données.

00110111111001111111111001

encapsulation :

01111110001101111110001111101110010111111 0

fanion **transparence** **fanion**

Délimiteurs et synchronisation : Violation du codage

- Exemple : Ethernet utilise un marqueur de début de trame et effectue une violation du codage Manchester pour détecter la fin de trame.

Contrôle d'accès au media

- Dans une liaison multipoint plusieurs stations utilisent le même support de transmission.
- Lorsque deux stations (ou plus) envoient des données (trames) simultanément sur le même support → il y a une collision (interférence).
- Physiquement : une collision signifie que les signaux qui représentent les données sont mélangés et on arrive pas à reconnaitre l'information.
- Les données doivent être retransmis ultérieurement.
- Il existe plusieurs protocoles de la sous-couche MAC : ALOHA, CSMA …

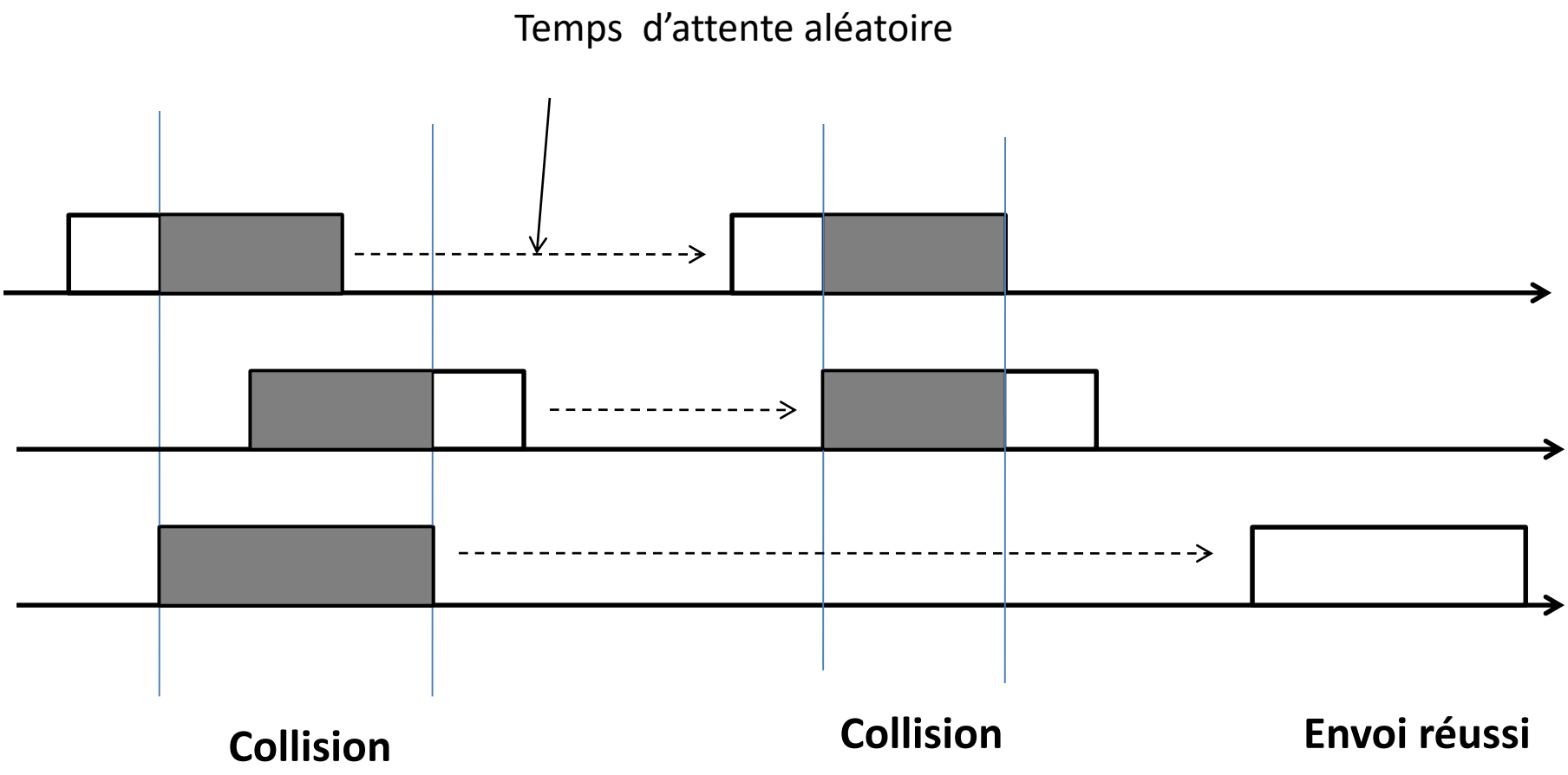
Méthode ALOHA

- Origine : l'université de Hawai (1972) a élaboré un système de communication radio ALOHA (ALOHA : bonjour en hawaïen) qui reliait les différentes îles de l'archipel.
- Problème : une seule fréquence disponible partagée entre l'ensemble des stations → comment permettre à l'ensemble d'émettre des données en même temps.

Méthode ALOHA

- Une station qui veut émettre une trame sur le réseau, commence immédiatement à le transmettre.
- Si deux émetteurs ou plus émettent en même temps → il y a collision (cela a engendré des collisions d'ondes radioélectriques).
- Les stations peuvent détecter les collisions. Alors elles doivent réémettre leur données ultérieurement.
- Les stations attendent une durée aléatoire avant de retransmettre la trame.
- Cette méthode utilise 18% du débit total dans le meilleur cas.

Exemple ALOHA



Méthode CSMA

- CSMA = Carrier Sense Multiple Access (Accès Multiple avec Ecoute de Porteuse).
- Basée sur l'écoute préalable du média de transmission avant l'émission d'une trame :
  - Si le canal est libre : transmettre la trame.
  - Si le canal est occupé : différer la transmission.
- CSMA est une méthode qui permet de réduire le nombre de collisions.
- Problème : il peut subsister des collisions en cours d'émission :
  - Lorsque deux stations émettent leurs données simultanément.
  - Lorsque l'émetteur écoute le support, il peut ne pas détecter la présence d'un signal à cause d'une distance trop grande.

Méthode CSMA/CD

- CSMA avec détection de collision : CSMA/CD (Collision Detection).
- Après l'émission de la trame, l'émetteur reste à l'écoute du support afin de détecter une éventuelle collision.
- Lors d'une collision la trame est alors réémise après un temps d'attente aléatoire.

Adresse MAC

- Une adresse MAC est un nombre codé sur 6 octets qui définit l'adresse physique (adresse matérielle) d'une carte réseau.
- C'est l'IEEE qui définit le format et l'assignation d'adresses MAC car elle doit être unique.

Adresse MAC

- L’adresse physique est composée de 2 parties.
- La première partie identifie le fabricant de la carte réseau (OUI-Organizationally Unique Identifier) et la seconde partie est un numéro qui n’a jamais été utilisé par ce même fabriquant UAA (Universally Administered Address).
- ID constructeur (24 bits) (0-23)
- numéro de série (24 bits) (24-47)
- ex : 00:0B:DB:1E:29:A1

Adresse MAC

- Exemples OUI :
  - 00 :00 :0C **Cisco**
  - 00 :05 :5D **D-Link**
  - 00 :06 :BC **3Com**
  - 00 :09 :5B **Netgear**
  - 00 :90 :69 **Juniper**
  - 00 :00 :B4 **Edimax**
  - http://www.kccommunications.com/htdocs/oui.htm
- Commandes pour trouver l'adresse MAC :
  - Windows : ***ipconfig /all***
  - Linux : ***ifconfig*** (champ Hwaddr)

Sous-couche LLC

Erreurs de transmission

- Les erreurs sont liées principalement aux supports de transmission.
- Un ou plusieurs bits d'information peuvent être changés durant la transmission des données.
- Les données peuvent être corrompues ou perdues.
- Les erreurs sont causées par :
  - L'interférence (Bruit)
  - La distorsion

Prévenir les erreurs de transmission

- Pour réduire les interférences :
  - Blinder les fils.
  - S'assurer que les câbles sont loin des sources d'interférence (Bruit).
- Pour réduire la distorsion :
  - Ajuster l'équipement de transmission et améliorer la qualité de la connexion.
  - Utiliser des amplificateurs et des répéteurs.
  - Utiliser des câbles de meilleur qualité.
- Le risque d'erreurs existe toujours, mais il ne doit pas dépasser un certain seuil 10^{-8} à 10^{-10}

Contrôle d'erreurs

- Il faut pouvoir détecter et corriger les erreurs.
- De façon générale pour transmettre **k** bits d'information, on ajoute **r** bits dit bits de contrôle.
- On parle de **code(n, k)** ou de mot de code.
- Les bits de contrôle sont calculés en fonction des bits de l'information.
- Au total on transmet **n= k + r** bits.
- À la réception, les bits de contrôle seront recalculer afin de s'assurer si l'information est bien reçue ou non.

Techniques de contrôle d’erreurs

- Il existe plusieurs méthodes de contrôle d’erreurs:
- Détection (code détecteur) :
  - Ce type de code permet de détecter le changement de un ou plusieurs bits d’information. Mais il n’a pas la possibilité de corriger ces erreurs.
- Détection et correction (code correcteur) :
  - Ce type de code permet de détecter le changement de un ou plusieurs bits d’information. En plus, il possède la capacité de corriger ces erreurs.

Détection d’erreurs

- Les techniques les plus utilisées pour la détection sont :
  - VRC (Vertical Redundancy Check) : Parité verticale.
  - LRC (Longitudunal Redundancy Check): Parité longitudinale.
  - CRC (Cyclic Redundancy Check) : Vérification polynomiale.

Parité verticale : VRC

- Le plus vieux mécanisme.
- Calculer la parité et rajouter un bit à l'information envoyé :
  - **Parité paire** : si le nombre de 1 dans l'information est paire alors le bit de parité est égale à 1, sinon 0
  - **Parité impaire** : si le nombre de 1 dans l'information est impaire alors le bit de parité est égale à 1, sinon 0
- Exemple :
  - si on utilise une parité impaire pour l'information **1100100** on rajoute **1**
  - l'information à envoyer est : **11001001**

Parité verticale : VRC

- La détection d'erreur avec le VRC consiste à :
  - **recalculer** le bit de parité à la réception et le comparer avec le bit de parité reçu.
- Exemple : l'information reçue est **11001001**
  - le bit de parité qui correspond à l'information : **1100100** est égal à **1** donc l'information reçue est correcte.
- Inconvénients :
  - On détecte l'erreur mais on peut pas savoir quel est le bit qui a changé.
  - Si le nombre de bits qui change est pair, alors il est impossible de détecter l'erreur. (**1100100** → **1110000**)

Parité longitudinale : LRC

- Appliquer le principe de la parité (paire ou impaire) aux colonnes d'un bloc de données.
- Exemple : envoi du message DATA

Caractère	Code ASCII
D	1000100
A	1000001
T	1010100
A	1000001
LRC	**1101111**

Parité longitudinale : LRC

- Plus efficace que le VRC.
- Impossible de détecter l'erreur si deux bits sont changés en même temps sur la même colonne.
- Pour plus d'efficacité rajouter un contrôle sur les lignes.

Caractère	ASCII	Bit de parité
D	1000100	1
A	1000001	1
T	1010100	0
A	1000001	1
LRC	1101111	1

CRC : Vérification polynomiale

- Rappel : Une information en binaire peut être écrite sous la forme polynomial suivant les puissance de 2

$$(1110)_2 = 1*2^3 + 1*2^2 + 1*2^1 + 0*2^0$$

- Dans le cas général :

$$(u_k u_{k-1} \ldots\ldots\ldots u_1 u_0)_2 = u_k.X^k + u_{k-1}.X^{k-1} + \ldots\ldots\ldots + u_1.X^1 + u_0.X^0 \text{ avec } u_i \in [0,1]$$

- Exemple : La suite 1100101 est représentée par le polynôme

$$1100101 = 1.X^6 + 1.X^5 + 0.X^4 + 0.X^3 + 1.X^2 + 0.X^1 + 1.X^0$$
$$= X^6 + X^5 + X^2 + 1$$

Calcul du CRC

- On choisit un polynôme appelé polynôme générateur **G(X)** de degré **n**
- Exemple : polynôme générateur $\mathbf{X^4 + X^2 + X}$ de degré **4**
- Soit une information sur **m** bits représentée sous la forme d'un polynôme **M(X)** de degré **m**
- Pour calculer le CRC :
  - multiplier le polynôme **M(X)** par $\mathbf{X^n}$ (n est le degré du polynôme générateur)
  - effectuer une division de $\mathbf{X^n.M(X)}$ par **G(x)**
  - on obtient le Quotient **Q(X)** et le reste **R(X)**

$$X^n\, M(X) = Q(X).G(X) + R(X)$$

  - Le CRC correspond au reste de la division **R(X)**
- Donc l'information à envoyer est égale à : **M(X).R(X)**

Calcul du CRC par des additions successives

- Soit **G(X)** un polynôme générateur de degré **n**. On le transforme en un mot binaire.
- **Exemple :**
  - Avec le polynôme générateur $\mathbf{X^4 + X^2 + X}$, on obtient **10110**
  - On ajoute **n** zéros au mot binaire à transmettre où **n** est le degré du polynôme générateur.
  - On souhaite transmettre le mot **11100111** en utilisant le polynôme générateur $\mathbf{X^4 + X^2 + X}$, on obtient alors **11100111**0000

- On va additionner itérativement (ou exclusif successifs) à ce mot, le mot correspondant au polynôme générateur jusqu'à ce que le mot obtenu soit inférieur au polynôme générateur.

- Ce mot obtenu correspond au CRC à ajouter au mot avant de l'émettre.

Exemple CRC

- Soit l'information 11100111 et le polynôme générateur $X^4 + X^2 + X$
- $G(X) = X^4 + X^2 + X$
- $M(X) = X^7 + X^6 + X^5 + X^2 + X^1 + 1$
- Multiplier M(X) par X^4
- $M(X).X^4 = X^{11} + X^{10} + X^9 + X^6 + X^5 + X^4$

  $= \mathbf{111001110000}$

Exemple CRC

```
1 1 1 0 0 1 1 1 0 0 0 0
1 0 1 1 0
-----------------------
0 1 0 1 0 1 1 1 0 0 0 0
  1 0 1 1 0
-----------------------
0 0 0 0 1 1 1 1 0 0 0 0
      1 0 1 1 0
-----------------------
0 0 0 0 0 1 0 0 0 0 0 0
        1 0 1 1 0
-----------------------
0 0 0 0 0 0 0 1 1 0 0 0
          1 0 1 1 0
-----------------------
0 0 0 0 0 0 0 0 1 1 1 0
```

Remarque :

Toutes les opération se font en effectuant des ou exclusifs (XOR)

$1 \oplus 1 = 0$

$1 \oplus 0 = 1$

$0 \oplus 1 = 1$

$0 \oplus 0 = 0$

Le code CRC = 1110

donc l'information à transmettre:

1110011 1110

Exemple CRC

```
11100111 1110
10110
-----
01010111 1110
 10110
-----
00001111110
    10110
-----
00000100110
     10110
-----
00000001010
       10110
-----
00000000000
```

A la réception, refaire la même opération.
Si le résultat est nul alors l'information est correcte.

Le reste de la division est nul donc l'information est correcte

Exercice CRC

- Soit le polynôme générateur $G(X)= X^4 + X^2 + X$
- Calculer le CRC pour les deux informations suivantes :

1111011101

1100010101

Normalisation des polynômes générateurs

- Le CCITT a recommandé un certain nombre de polynômes :

- $CRC-12 = x^{12} + x^{11} + x^{3} + x^{2} + x + 1$
- $CRC-16 = x^{16} + x^{15} + x^{2} + 1$
- $CRC-CCITT = x^{16} + x^{12} + x^{5} + 1$ (utilisé par HDLC)
- $CRC-32 = x^{32} + x^{26} + x^{23} + x^{22} + x^{16} + x^{12} + x^{11} + x^{10} + x^{8}$

$+ x^{7} + x^{5} + x^{4} + x^{2} + x + 1$ (Ethernet utilise un CRC-32)

Quelques protocoles de niveau 2

- Ethernet.
- HDLC : High-level Data Link Control.
- PPP : Point to Point Protocol (utilisé dans les connexions à Internet par modem).
- LAP : Link Access Procedure.

Le protocoles HDLC

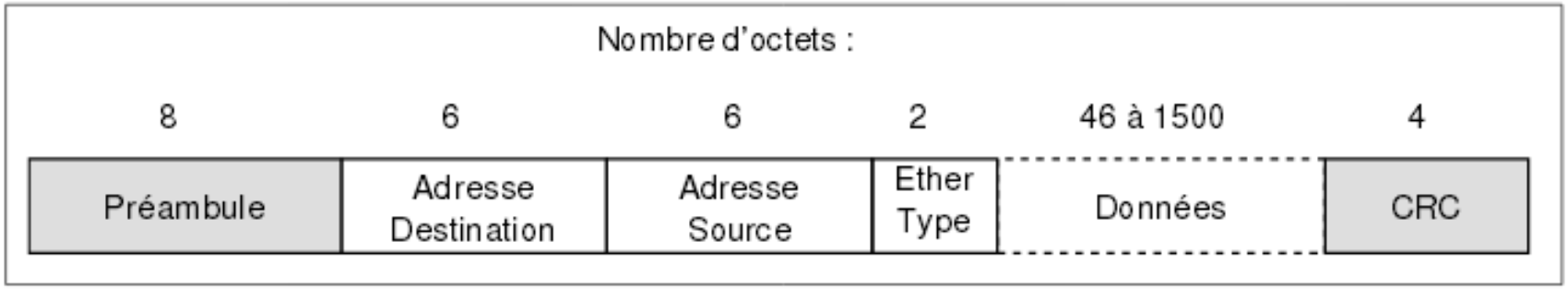
- Utilisé dans le GSM et les liaisons série entre routeurs Cisco
- Format des trames binaires utilisées par HDLC:

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 le DTE destinataire.
- Commande = informations nécessaires à l'interprétation de la trame. Il existe 3 types de trames : **trame d'information (données), trame de supervision et trame non numéroté.**
- Le contrôle d'erreur est réalisé par un code CRC basé sur le polynôme générateur $G(X)= X^{16} + X^{12} + X^5 + 1$

Ethernet

- Equipe actuellement la quasi-totalité des réseaux locaux d'entreprise (LAN)
- Format de la trame Ethernet V2 :



- Préambule (8 octets) : annonce le début de la trame et permet aux récepteurs de se synchroniser. Il contient 8 octets dont la valeur est **10101010** (on alterne des 1 et des 0), sauf pour le dernier octet dont les 2 derniers bits sont à 1.

Ethernet

- Adresse Destination et Source (6 octets): adresse MAC de l'interface (carte réseau) Ethernet destinataire (resp. source) de la trame.
- EtherType (2 octets) : type de trame, indique le protocole de la couche réseau encapsulé dans la trame.
- Données (46 à 1500 octets) : les données véhiculées par la trame.
- CRC (Cyclic Redundancy Code) : le contrôle d'erreur est réalisé par un code CRC basé sur le polynôme générateur CRC-32

$$\mathrm{CRC\text{-}32} = x^{32} + x^{26} + x^{23} + x^{22} + x^{16} + x^{12} + x^{11} + x^{10} + x^{8} + x^{7} + x^{5} + x^{4} + x^{2} + x + 1$$

Réseaux informatiques

Chapitre 5 – Couche réseau

Mustapha Anwar BRAHAMI

ESSA Tlemcen

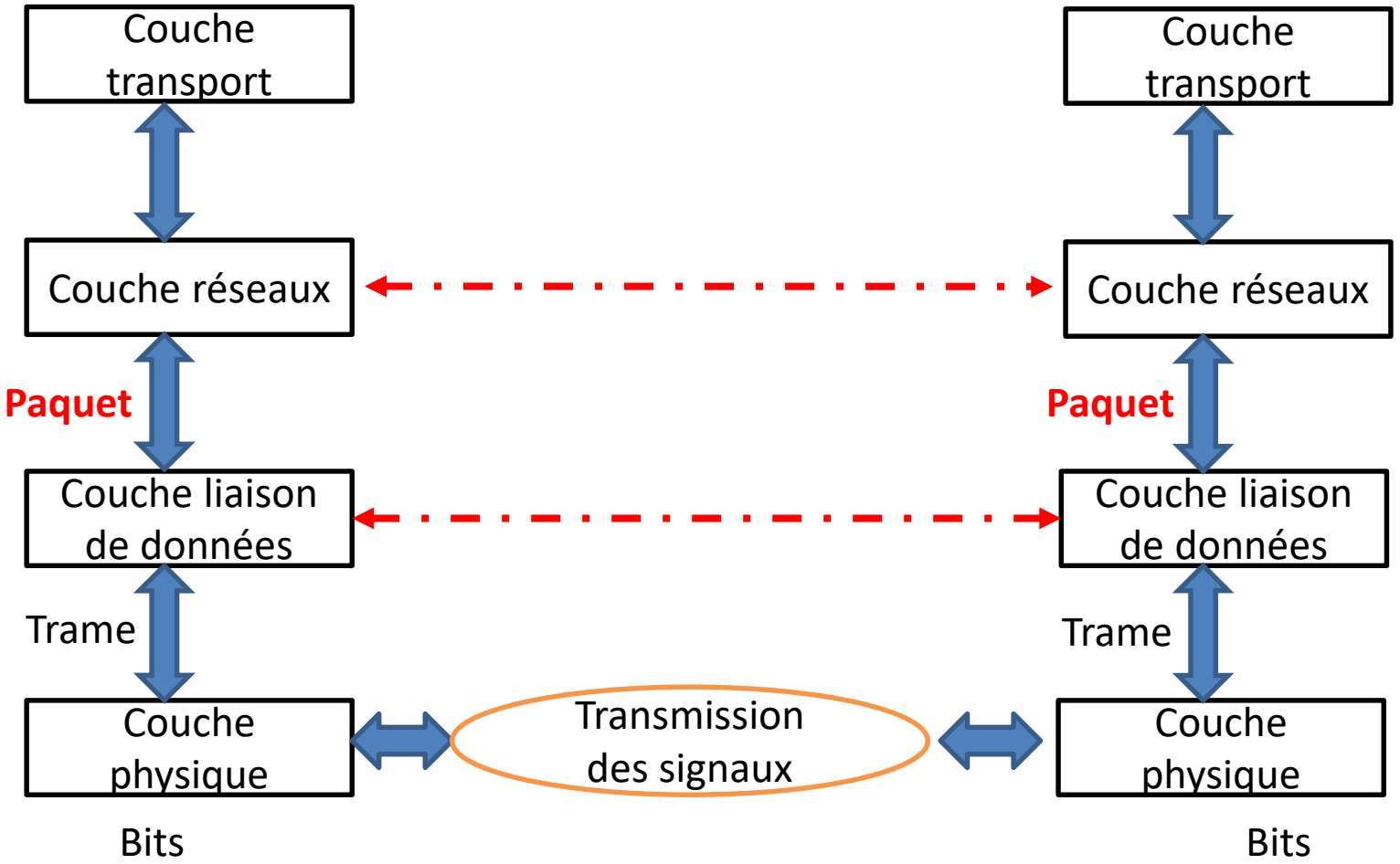
Références bibliographiques

Ce cours est construit à partir d'un certains nombres de support de cours disponibles sur le net. L'usage de ce composite ne peut être qu'académique :

- DORDOIGNE, J. (2015). *Réseaux informatiques - Notions fondamentales (6ième édition)*. ENI. ISBN : 9782746093928
- LEGRAND, R. (2014). *Notions de base sur les réseaux : 1er module de préparation à la certification CCNA 200-120*. ENI. ISBN : 9782746092136
- DROMARD, D. (2006). *Architecture des réseaux*. Pearson. ISBN : 9782744076640
- LOHIER, S. (2010). *Le réseau Internet : des services aux infrastructures*. Dunod. ISBN : 9782100546046
- CISCO Systems. *Notions de base sur les réseaux*. CCNA Exploration Fr V 4.0
- FERRAND, P. (2013). *Réseaux*. INSA de Lyon. http://www.ferrand.cc/pdfs/cours_reseaux.pdf
- DUVALLET, C. (2016). *Open System Interconnetion (OSI)*. Université duHavre.http://litis.univlehavre.fr/~duvallet/enseignements/Cours/M1INFO/Reseau/MI-Cours-Reseau-Cours2.pdf
- Cours couche réseau. ENS Kouba.

Couche réseau

- L'unité d'information associée à la couche 3 du modèle OSI est le **paquet**.



Rôle de la couche réseau

- Achemine les paquets de données entre l'émetteur et le destinataire à travers différents réseaux (maillage réseau).
- La couche réseau offre deux fonctionnalités de base :
  - L'adressage (Identification des machines) : chaque machine doit être dotée d'une adresse logique unique dans un réseau.
  - Le routage : la couche réseau permet de retrouver une machine dans un réseau grâce à une route précisant comment la machine peut être atteinte.

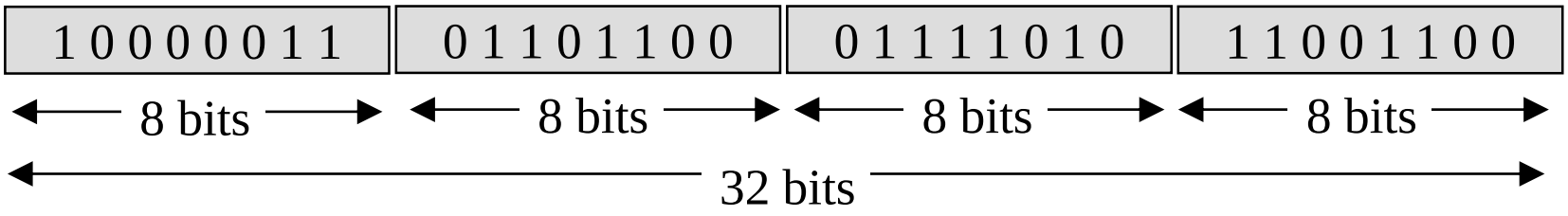
Adressage logique IPv4

Principe de l’adressage

- Chaque hôte (machine) dispose d’une adresse unique.
- L’adresse est une adresse logique et non physique (peut être modifiée).
- Les adresses sont groupées par rapport au numéro du réseau (adresse réseau).

Adresse IP

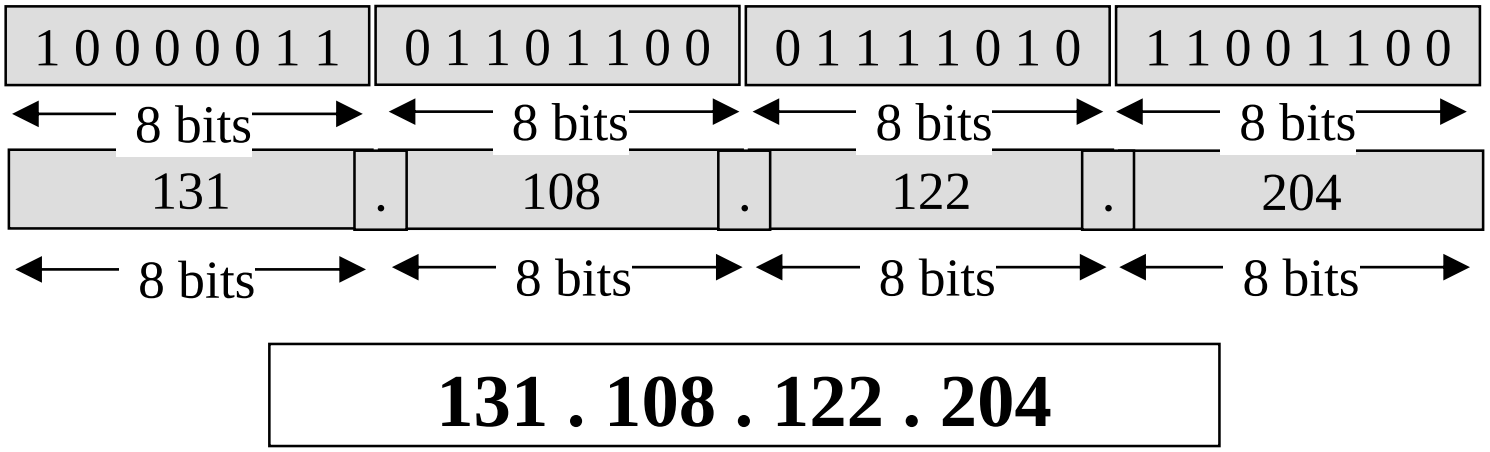
- Une adresse IP est codée sur 32 bits (4 octets).
- Chaque combinaison (2^{32} combinaisons) représente une adresse.



- Il est pratiquement impossible de mémoriser 32 bits → une adresse IP est représentée dans un format décimal avec 4 nombres séparés par des points.
- On parle de "notation décimale pointée".

Notation décimale pointée des adresses IP

- Chaque 8 bits de l'adresse représente un nombre décimal.
- Ce nombre décimal représente une valeur entre 0 à 255.
- **Exemple 1 :**



- **Exemple 2 :** L'adresse **131.108.122.264** est non valide puisque le dernier nombre est supérieur a 255.

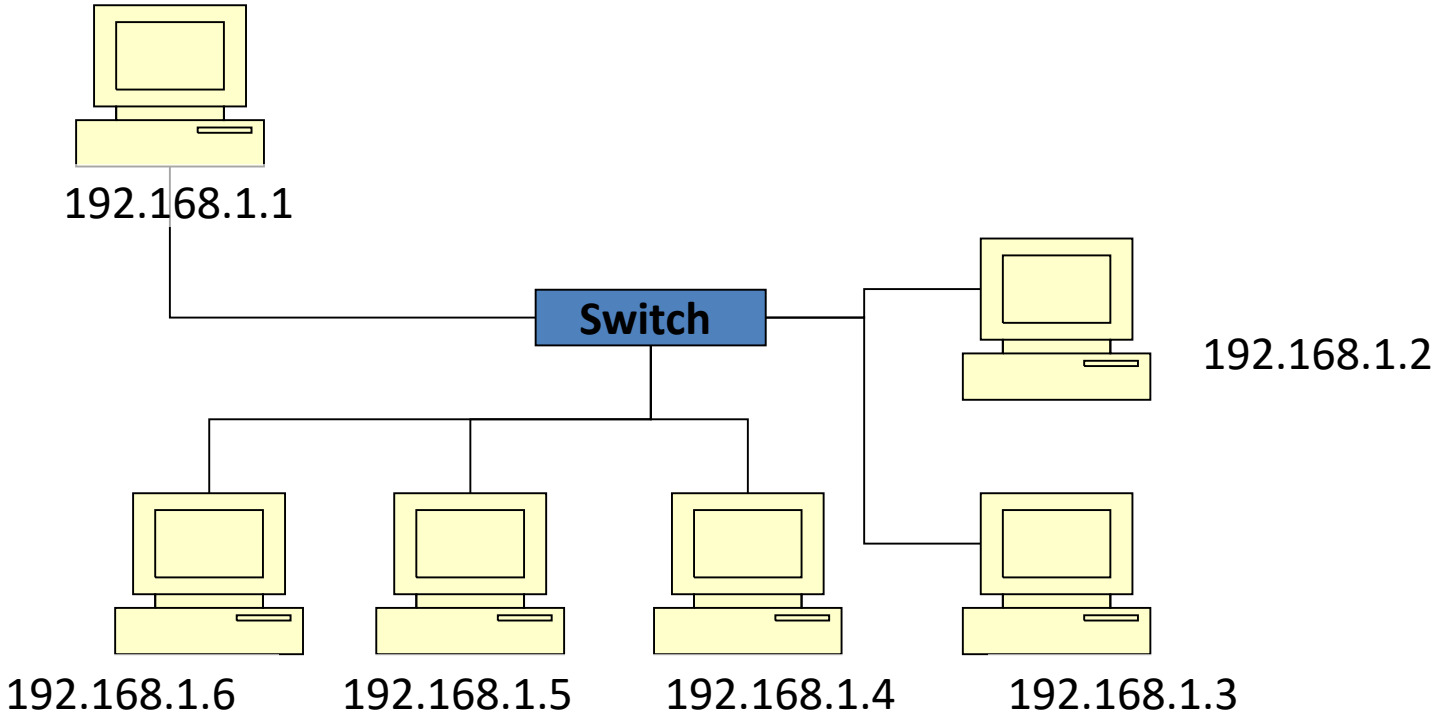
Champs d'une adresse IP

- Une adresse IP comprend deux parties :
  - Un **numéro de réseau (NET-ID)**: une adresse globale pour identifier un réseau, cette adresse est commune à toutes les machines de ce réseau.
  - Un **numéro de machine (hôte)** : identifier une machine dans un réseau.

- **Exemple :** soit l'adresse 131.108.122.204, si on considère **k=16 et n=16** alors :
  - NET-ID : **131.108**
  - HOST : **122.204**

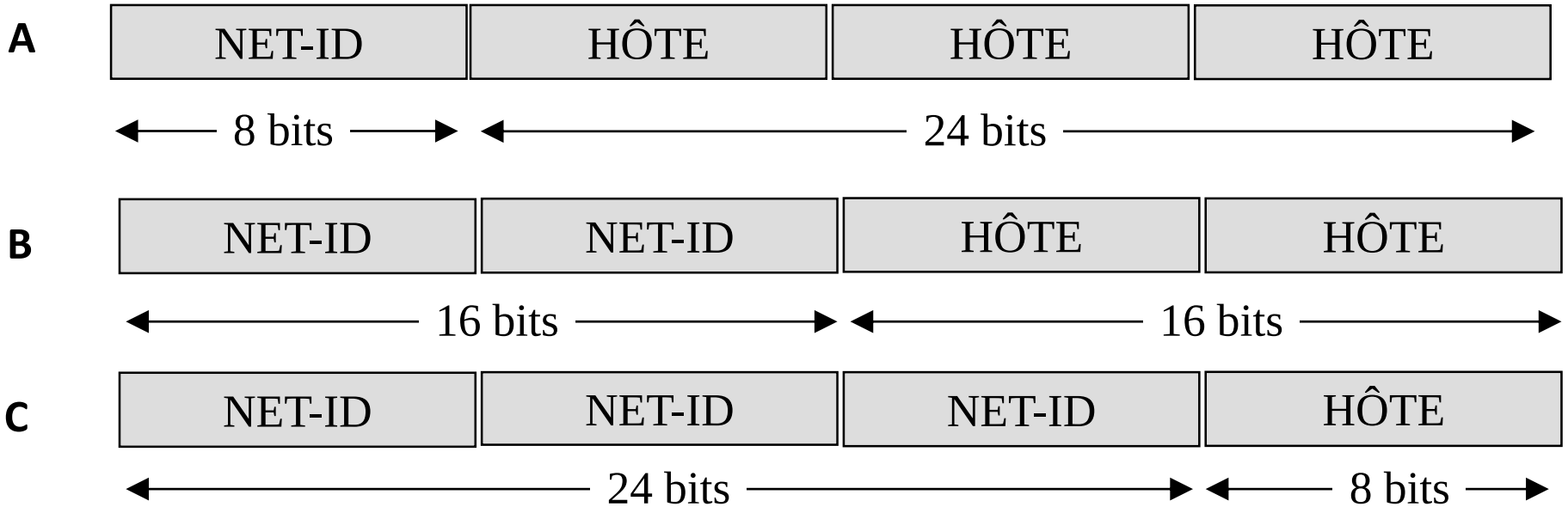
Exemple

- Soit le réseau ayant le numéro **192.168.1.0**
- Les machines de ce réseau possèdent les adresses suivantes : **192.168.1.1**, **192.168.1.2**, **192.168.1.3**, **192.168.1.4**, **192.168.1.5**, **192.168.1.6**



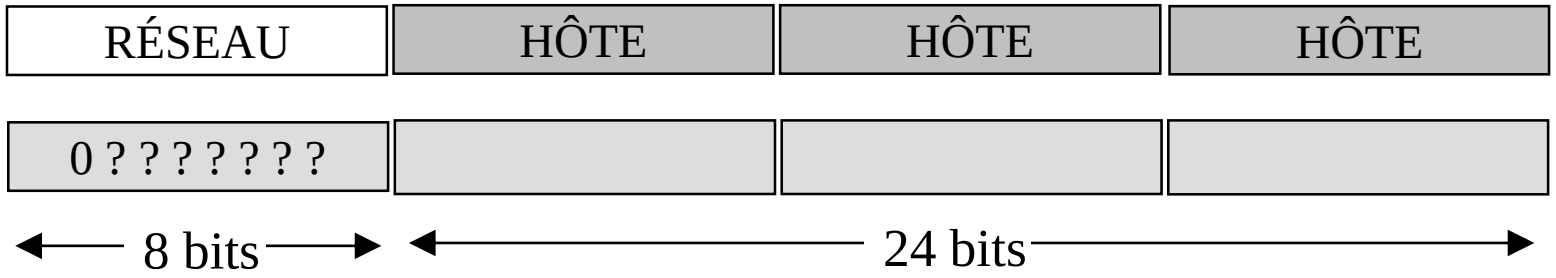
Classes d'adresse IP

- La taille de la partie réseau (net-id) détermine la classe de l'adresse IP.
- Les adresses IP sont classées en 3 classes :



Adresse IP de classe A

- Le premier octet est réservé au réseau, les 3 octets (24 bits) suivants sont réservés aux hôtes.
- Le premier octet d'une adresse IP de classe A commence toujours par le bit **0** (il reste 7 bits).



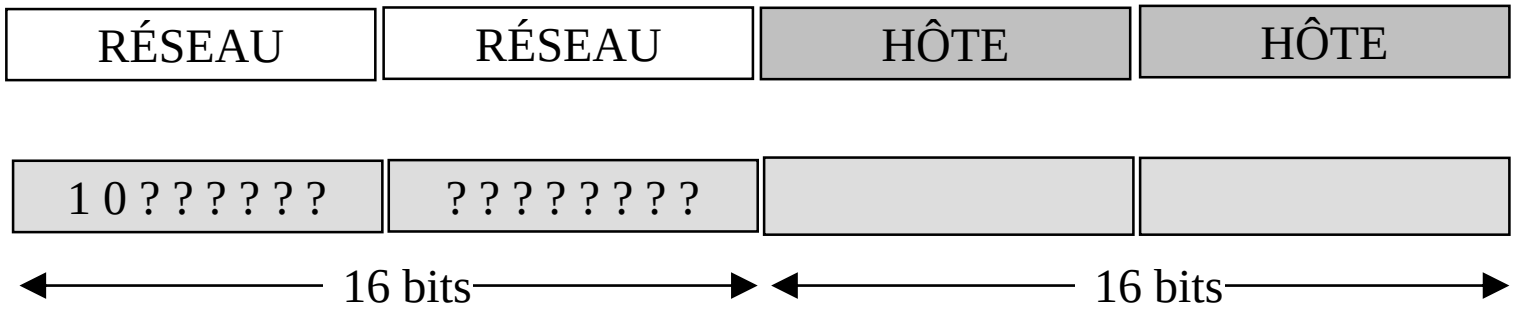
- **Nombre de réseaux disponibles** : 2^7 = 128 réseaux.
- **Nombre d'hôtes disponibles** : 2^{24} - 2 = 16 777 214 hôtes.
- Exemple :

  90.25.48.10 correspond à une adresse de classe **A**.

  01011010 00011001 00110000 00001010

Adresse IP de classe B

- Les 2 premiers octets sont réservés au réseau, les 2 octets (16 bits) suivants sont réservés aux hôtes.
- Le premier octet d'une adresse IP de classe B commence toujours par la séquence de bit **10** (il reste 14 bits).



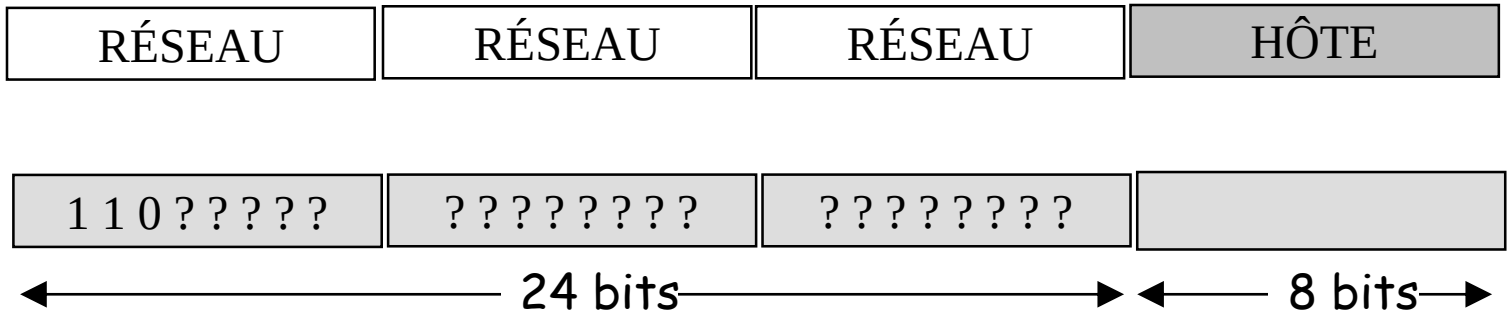
- **Nombre de réseaux disponibles** : 2^{14} = 16 384 réseaux.
- **Nombre d'hôtes disponibles** : 2^{16} - 2 = 65 534 hôtes.
- **Exemple :**

  130.100.20.10 correspond à une adresse IP de la classe **B**.

  10000010 01100100 00010100 00001010

Adresse IP de classe C

- Les 3 premiers octets sont réservés au réseau, l'octet (8 bits) suivant est réservé aux hôtes.
- Le premier octet d'une adresse IP de classe C commence toujours par la séquence de bits **110** (il reste 21 bits).



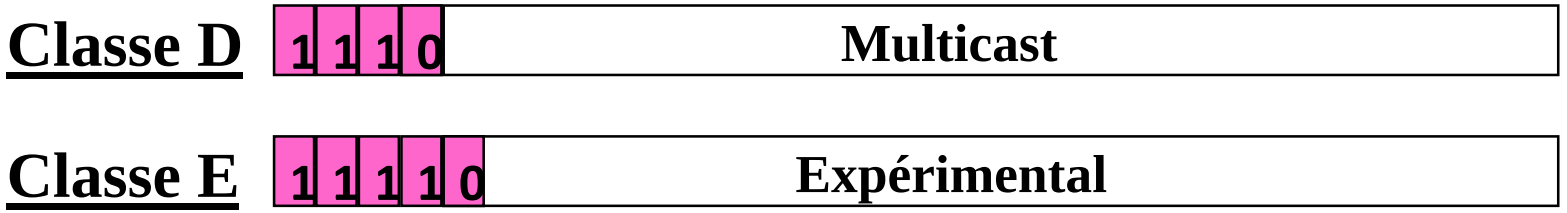
- **Nombre de réseaux disponibles** : 2^{21} = 209 752 réseaux.
- **Nombre d'hôtes disponibles** : 2^{8} - 2 = 254 hôtes.
- **Exemple :**

  192.5.5.11 correspond à une adresse de classe **C**.

  11000000 00000101 00000101 00001011

Classes d'adresses IP particulières

- Il existe deux autres classes d'adresses IP particulières :
  - La classe D : réservé pour les communications multicast (communication en groupe)
  - La classe E : les adresses de la classe E sont réservés pour les expérimentations.



- **Exemple :**
  - L'adresse 226.5.5.11 est de classe D

    11100010 00000101 00000101 00001011
  - L'adresse 242.5.5.11 est de classe E

    11110010 00000101 00000101 00001011

Intervalle d'adresses IP de classe A

- de **0**0 00 00 01 . 00 00 00 00 . 00 00 00 00 . 00 00 00 00
- à **0**1 11 11 11 . 11 11 11 11 . 11 11 11 11 . 11 11 11 11
- La plage d'adresses possibles de: **1.0.0.0** à **126.255.255.255**
- **Remarque :**
  - L'adresse **0.b.c.d** n'existe pas.
  - L'adresse **127.b.c.d** : tq b, c et d sont des nombres [0,255] représente une adresse de boucle de retour (loop back).
  - Dans ce cas, le paquet est envoyé vers le même hôte, sans être transmis sur le réseau.
  - Elle est utilisée même s'il n'y a pas d'interface réseau physiquement sur la machine.

Intervalles d’adresses IP de classe B et C

- Classe B :
  - de **10** 00 00 00 . 00 00 00 00 . 00 00 00 00 . 00 00 00 00
  - à **10** 11 11 11 . 11 11 11 11 . 11 11 11 11 . 11 11 11 11
  - La plage d’adresses possibles : de **128.0.0.0** à **191.255.255.255**

- Classe C :
  - de **11 0**0 00 00 . 00 00 00 00 . 00 00 00 00 . 00 00 00 00
  - à **11 0**1 11 11 . 11 11 11 11 . 11 11 11 11 . 11 11 11 11
  - La plage d’adresses possibles : de **192.0.0.0** à **223.255.255.255**

Adresse de réseau

- Dans le cas ou la partie hôte comporte uniquement des **0,** alors cette adresse correspond à l'adresse du réseau (identité du réseau).
- Une adresse réseau ne peut pas être attribuée à une machine (adresse non valide).
- **Exemple :**
  - Dans l'adresse de classe A :
    90.25.48.10 : l'adresse **90.0.0.0** correspond à une adresse de réseau.
  - Dans l'adresse de classe B :
    130.100.20.10 : l'adresse **130.100.0.0** correspond à une adresse de réseau.
  - Dans l'adresse de classe C :
    192.5.5.11 : l'adresse **192.5.5.0** correspond à une adresse de réseau.

- L'adresse qui comporte uniquement des 0 dans la partie réseau et hôte (**0.0.0.0**) désigne tout les réseaux (route par défaut cf. routage).

Adresse de broadcast

- Adresse de diffusion (broadcast) : On parle de diffusion lorsqu'une source envoie des données à toutes les unités d'un réseau.
- Toutes les machines du même réseau reçoivent le paquet de données.
- Quand une adresse ne contient que des **1** dans la partie hôte. Elle est appelée adresse de diffusion (broadcast).
- Une adresse de broadcast ne peut pas être attribué a une machine (adresse non valide).
- **Exemple :**
- L'adresse de diffusion correspondant à l'adresse de Classe A **90.25.48.10** est **90.255.255.255**
- L'adresse de diffusion correspondant à l'adresse de Classe B **130.100.20.10** est **130.100.255.255**
- L'adresse de diffusion correspondant à l'adresse de Classe C **192.5.5.11** est **192.5.5.255**

Masque de réseau

- C’est une combinaison de bits utilisée pour décrire la portion d’une adresse qui désigne le réseau et la portion qui désigne l’hôte.
- Il est calculé comme suit :
  - Exprimez l’adresse IP au format binaire.
  - Remplacez tous les bits de **la portion réseau de l’adresse par des 1**.
  - Remplacez tous les bits de **la portion hôte de l’adresse par des 0**.
  - Enfin, convertissez l’adresse binaire au format décimal.

Le masque par défaut pour:

- **Classe A: 255.0.0.0 → /8**
- **Classe B: 255.255.0.0 → /16**
- **Classe C: 255.255.255.0 →/24**

Exemple 1 : classe A

- Soit l'Adresse IP : **12.30.10.2** avec le masque de réseau : **255.0.0.0 → 12.30.10.2 /8**
- **Informations sur le réseau :**
  - La classe : **A** Nombre de bits pour réseau : **8** Nombre de bits d'Hôtes : **24**
  - Adresse réseau (Identité de réseau) : **12.0.0.0**
  - Adresse broadcast : **12.255.255.255**
  - Adresse valide du premier Hôte du réseau : **12.0.0.1**
  - Adresse valide du dernier Hôte du réseau : **12.255.255.254**

Exemple 2 : classe B

- Soit l'adresse IP : **172.30.10.2** avec le masque de réseau : **255.255.0.0 → 172.30.10.2/16**
- **Informations réseau :**
  - La classe : **B** Nombre de bits pour réseau : **16** Nombre de bits d'Hôtes : **16**
  - Adresse réseau (Identité de réseau) : **172.30.0.0**
  - Adresse broadcast : **172.30.255.255**
  - Adresse valide du premier Hôte du réseau : **172.30.0.1**
  - Adresse valide du dernier Hôte du réseau : **172.30.255.254**

Exemple 3 : classe C

- Soit l'adresse IP : **192.130.10.2** avec le masque réseau : **255.255.255.0 → 192.130.10.2/24**
- **Informations réseau :**
  - La classe : **C** Nombre de bits pour réseau : **24** Nombre de bits d'Hôtes : **8**
  - Adresse réseau (Identité de réseau) : **192.130.10.0**
  - Adresse broadcast : **192.130.10.255**
  - Adresse valide du premier Hôte du réseau : **192.130.10.1**
  - Adresse valide du dernier Hôte du réseau : **192.130.10.254**

Résumé

Classes d'adresses IP

Classe d'adresse	Plage du premier octet (décimale)	Bits du premier octet (les bits verts ne changent pas)	Parties réseau(N) et hôte (H) de l'adresse	Masque de sous-réseau par défaut (décimal et binaire)	Nombre de réseaux et d'hôtes possibles par réseau
A	1-127**	00000000-01111111	N.H.H.H	255.0.0.0	126 réseaux (2^7-2) 16 777 214 hôtes par réseau (2^24-2)
B	128-191	10000000-10111111	N.N.H.H	255.255.0.0	16 384 réseaux (2^14) 65 534 hôtes par réseau (2^16-2)
C	192-223	11000000-11011111	N.N.N.H	255.255.255.0	2 097 150 réseaux (2^21) 254 hôtes par réseau (2^8-2)
D	224-239	11100000-11101111	S.O. (multidiffusion)		
E	240-255	11110000-11111111	S.O. (expérimental)		

** Les réseaux 0.0.0.0 et 127.0.0.0 ne sont pas valides

Exercice 1

- Complétez le tableau suivant en indiquant :
  - La classe de chaque adresse IP.
  - Si les adresses IP sont valides ou non (justifier votre réponse).

Adresse	Classe	Valide ou non	Justification
150.100.255.255			
175.100.255.18			
195.234.253.0			
100.0.0.23			
188.258.221.176			
127.34.25.189			

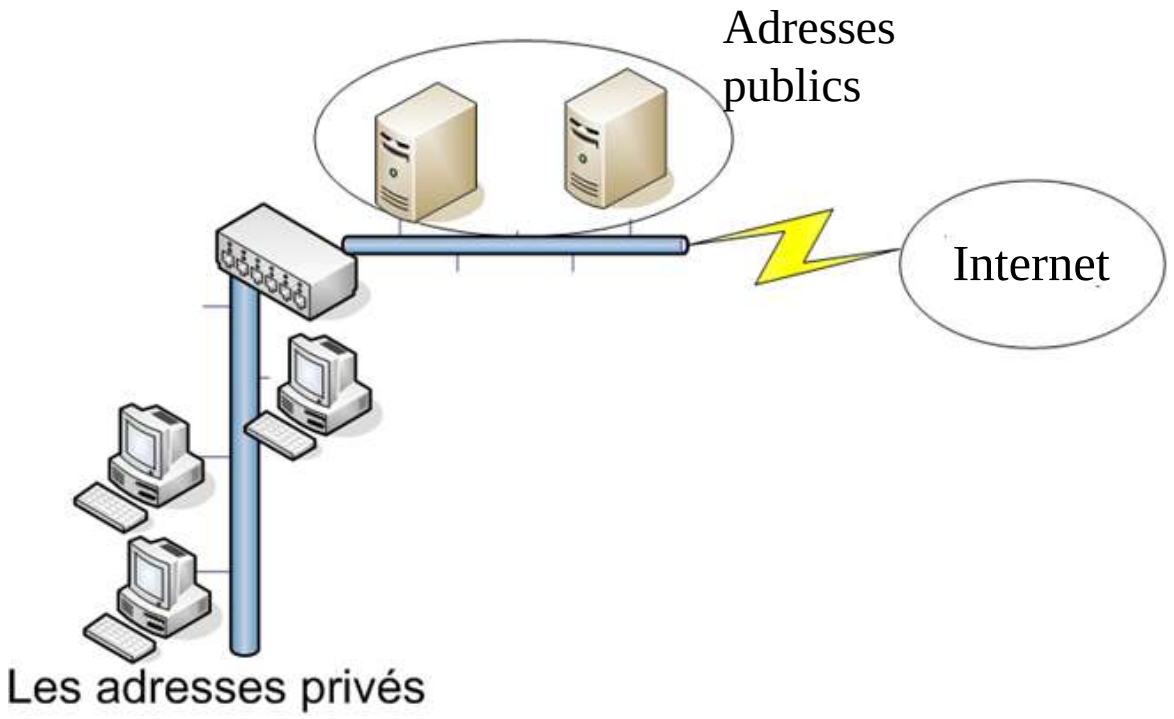
Exercice 2

- Compléter le tableau suivant :

Adresse IP hôte	Classe d'adresses	Adresse réseau	Partie hôte	Adresse de broadcast	Masque de réseau par défaut
216.14.55.137					
123.1.1.15					
150.127.221.244					
194.125.35.199					
175.12.239.244					

Adresses IP publiques

- Les adresses IP publics sont attribuées aux entreprises et aux organismes par l'**ICANN** (Internet Corporation for Assigned Names and Numbers) pour assurer **l'unicité de ces adresses**.
- Ces adresses IP sont dites **publics (visibles sur Internet)**.
- Les adresses publiques sont uniques.
- Pour connaitre son adresse IP public : www.adresseip.com, www.whatismyip.com



Adresses IP privées

- Utilisées dans un réseau privé (local).
- Si les machines d'un réseau n'ont pas besoin d'être visibles à l'extérieur (Internet).
- Cela ne nécessite pas d'avoir une adresse IP public → on peut alors utiliser des adresses privées (qui peuvent être réutiliser dans d'autres réseaux).
- Les plages d'adresses IP privées :
  - **1** réseau de classe A : **10.0.0.0** à **10.255.255.255**
  - **16** réseaux de classe B : **172.16.0.0** à **172.31.0.0**
  - **256** réseaux de classe C : **192.168.0.0** à **192.168.255.0**

Attribution d'adresse IP statique/dynamique

- Il existe plusieurs façons d'attribuer une adresse IP à un ordinateur :
- Certaines machines possèdent toujours la même adresse (adresse statique) : cette adresse est attribuée d'une manière manuelle (en utilisant une commande ou via une interface graphique) :
  - Linux : ***ifconfig eth0 192.168.0.5 netmask 255.255.255.0***
- Certaines machines possèdent une adresse qui change à chaque démarrage (adresse dynamique) : cette adresse est attribuée d'une façon dynamique et automatique par une autre machine (serveur DHCP : Dynamic Host Configuration Protocol) :
  - Linux : ***iface eth0 inet dhcp***

Les sous-réseaux

Création de sous-réseaux

- Le principal problème des adresses IP est le gaspillage de l'espace d'adressage → des adresses réservées mais non attribuées.
- Par exemple :
  - Si on dispose de 50 machines dans un réseau → cela nécessite 50 adresses.
  - La classe la plus adéquate est la classe C (par exemple 193.220.12.0) qui dispose de 254 hôtes → utiliser 50 adresses seulement.
  - Mais le reste des adresses (204 adresses) sont inutilisées et ne peuvent pas être affectées ailleurs puisque l'adresse réseau est déjà attribuée.
- Donc pourquoi ne pas utiliser les adresses d'un réseau ayant une capacité qui répond juste au besoin sans gaspiller les adresses, cela revient à prendre une partie du réseau global au lieu de prendre la totalité des adresses offertes par ce réseau.

Problèmes ?

- Comment déterminer les sous-réseaux (comment déterminer l'adresse de chaque sous réseau).
- Comment calculer le masque des sous-réseaux.
- Comment calculer l'intervalle des adresses valides de chaque sous-réseau.
- Comment calculer l'adresse du broadcast de chaque sous-réseau.

Principe du découpage en sous-réseaux

- Pour effectuer ce découpage :
- Prendre **n** bits de la partie **hôte** → ces bits doivent être réattribués à la **partie réseau** dans l'adresse.
- Le nombre de bits a empruntés dépond du nombre de **sous-réseaux** qu'on veut avoir et le nombre d'**hôtes** dans chaque sous-réseau.
- Exemples :
  - Si on veut avoir deux sous-réseaux alors emprunter 1 bit (2^1).
  - Si on veut avoir 4 sous-réseau, emprunter 2 bits (2^2).
  - Si on veut avoir 7 sous-réseaux alors emprunter 3 bits (2^3= sous réseaux) →utiliser uniquement 7.

Principe du découpage en sous-réseaux

- Cette opération est souvent appelée « emprunt » de bits.
- L'emprunt se fait toujours à partir du bit d'hôte situé le plus à gauche.
- Chaque combinaison des bits empruntés représente un sous-réseaux (2^n sous-réseaux).
- Le nombre de bits qui reste détermine le nombre d'adresses utilisables dans le sous-réseau.
- ($2^{\text{nombre de bits hôtes restants}}$) – 2 = adresses utilisables (nombre d'hôtes).
- La soustraction correspond aux deux adresses réservées que sont l'adresse du réseau et l'adresse de broadcast du réseau.

Exemple

- Soit l'adresse du réseau de la classe C : **192.55.12.0**
- En binaire : **11000000.00110111.00001100.00000000**
- Supposant qu'on veut avoir 4 sous-réseaux :
  - Dans ce cas on prend deux bits de la partie hôte (chaque sous-réseau comportera $2^6 - 2 = 62$ hôtes)
  - Le premier sous-réseau : **11000000.00110111.00001100.00000000**

    192.55.12.0
  - Le deuxième sous-réseau : **11000000.00110111.00001100.01000000**

    192.55.12.64
  - Le troisième sous-réseau : **11000000.00110111.00001100.10000000**

    192.55.12.128
  - Le quatrième sous-réseau : **11000000.00110111.00001100.11000000**

    192.55.12.192

Masque de sous-réseaux

- Lorsqu'on utilise les sous-réseaux, **le masque réseau par défaut n'est plus valable**, puisque nous avons rajouté **des bits supplémentaires au net-id (partie réseau)**.
- La nouvelle valeur du masque pour les sous-réseaux est calculée comme suit :
  - Prendre le masque par défaut du réseau initial
  - Compléter les bits empruntés de la partie hôte par des **1**
  - et laisser les bits restant de la partie hôte à **0**
- Exemple :
  - Avec deux sous-réseaux, pour l'adresse de classe C : **192.55.12.0**
  - Masque par défaut (255.255.255.0) : **11111111.11111111.11111111.00000000**
  - Le masque des nouveaux sous-réseaux : **11111111.11111111.11111111.10000000** → **255.255.255.128** ou indiquer juste le nombre de bits à 1 → **/25**
  - Donc le premier sous-réseau : **192.55.12.0 /25**
  - Le deuxième sous-réseaux: **192.55.12.128 /25**

Exemple

- Soit l'adresse du réseau de la classe C : **192.55.12.0**
- Supposant qu'on veut avoir 4 sous-réseaux :
  - Nombre de bits empruntés = 2 bits
  - Le nouveau masque : 11111111.11111111.11111111.11000000 → 255.255.255.192
  - Le premier sous-réseau : **192.55.12.0 /26**
  - Le deuxième sous-réseau : **192.55.12.64 /26**
  - Le troisième sous-réseau : **192.55.12.128 /26**
  - Le quatrième sous-réseau : **192.55.12.192 /26**

Adresse de broadcast pour les sous-réseaux

- L'adresse de broadcast est une adresse dont la partie hôte ne contient que des 1.
- Dans le cas des sous réseaux l'adresse du broadcast n'est pas la même pour tout les sous-réseaux.
- Pour calculer l'adresse de broadcast d'un sous réseaux :
  - Ecrire l'adresse de ce sous-réseau en binaire
  - Remplir la partie hôte uniquement avec des 1
  - Et traduire par la suite en décimal

Exemple

- Le premier réseaux 192.55.12.0 :
  11000000.00110111.00001100.**00**000000
  L'adresse de broadcast 11000000.00110111.00001100.00**111111** → 192.55.12.63

- Le deuxième sous-réseau 192.55.12.64 :
  11000000.00110111.00001100.**01**000000
  11000000.00110111.00001100.01**111111** → 192.55.12.127

- Le troisième sous-réseau 192.55.12.128 :
  11000000.00110111.00001100.**10**000000
  11000000.00110111.00001100.10**111111** → 192.55.12.191

- Le quatrième sous-réseau 192.55.12.192 :
  11000000.00110111.00001100.11000000
  11000000.00110111.00001100.11**111111** → 192.55.12.255

Intervalle des adresses valides

- Soit l'adresse du réseau de la classe C : **192.55.12.0**
- Supposant qu'on veut avoir 4 sous-réseaux :
  - Dans ce cas on prend deux bits de la partie hôte (chaque sous-réseau comportera $2^6 - 2 = 62$ hôtes)

  - Le premier sous-réseau : **11000000.00110111.00001100.00000000**
    192.55.12.0 (adresses valides : 192.55.12.1 → 192.55.12.62)

  - Le deuxième sous-réseau : **11000000.00110111.00001100.01000000**
    192.55.12.64 (adresses valides : 192.55.12.65 → 192.55.12.126)

  - Le troisième sous-réseau : **11000000.00110111.00001100.10000000**
    192.55.12.128 (adresses valides : 192.55.12.129 → 192.55.12.190)

  - Le quatrième sous-réseau : **11000000.00110111.00001100.11000000**
    192.55.12.192 (adresses valides : 192.55.12.193 → 192.55.12.254)

Exercice 4

- L'adresse réseau de votre organisme est **150.193.0.0**
- Vous avez besoin de **50** sous-réseaux. Chaque sous-réseau comporte **750** hôtes.

- Quelle est la classe d'adresse ?
- Quel est le masque par défaut ?
- Combien de bits faut-il emprunter à la partie hôte de l'adresse réseau pour créer au moins 50 sous-réseaux ayant chacun au moins 750 hôtes ?
- Quel sera le masque de sous-réseau.
- Donnez, pour les 4 premiers sous-réseaux, la plage des adresses machines et l'adresse de broadcast.

Exercice 3

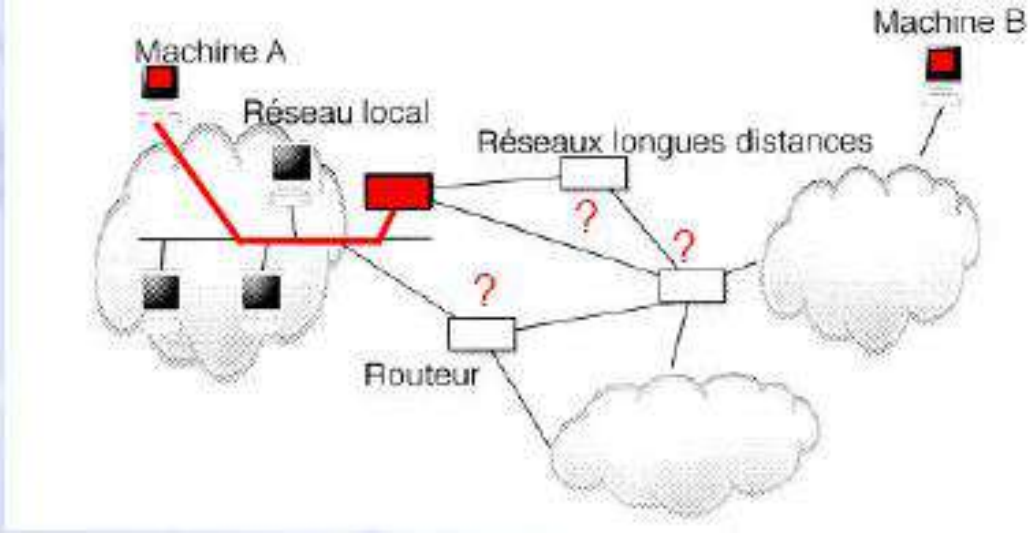
- Soit les trois machines A, B et C ayant pour adresses :
  - A : 192.168.0.133 / 25
  - B : 192.168.0.200 / 27
  - C : 192.168.0.220 / 26

- Donner l'adresse de sous-réseau de chaque machine et indiquez la valeur du masque de sous-réseau sous la forme décimal?
- Combien de machines existent dans le réseau des machines A, B et C ?

Le routage IP

Problématique de routage

- **Objectif** : Acheminer des paquets IP d'une machine source A vers une machine destination B.
- **Problématique** : Comment atteindre la machine B en connaissant son adresse IP?



Routage IP : définition

- Déterminer (choisir) la route par lesquels les paquets sont transmis de la source à la destination à l'aide d'équipements appelés **routeurs.**
- Processus basé sur une table de routage IP (routing table) contenant les informations relatives aux différentes destinations possibles et à la façon de les atteindre.

Paquet IP

Bit 0 - 7	Bit 8 - 15	Bit 16 - 23	Bit 24 - 31
Version/IHL	Type de service	Longueur totale	
Identification (fragmentation)		*flags* et *offset* (fragmentation)	
Durée de vie(TTL)	Protocole	Somme de contrôle de l'en-tête	
Adresse IP source			
Adresse IP destination			
Type de message	Code	Somme de contrôle	
Bourrage ou données			
Données (*optionnel et de longueur variable*)			

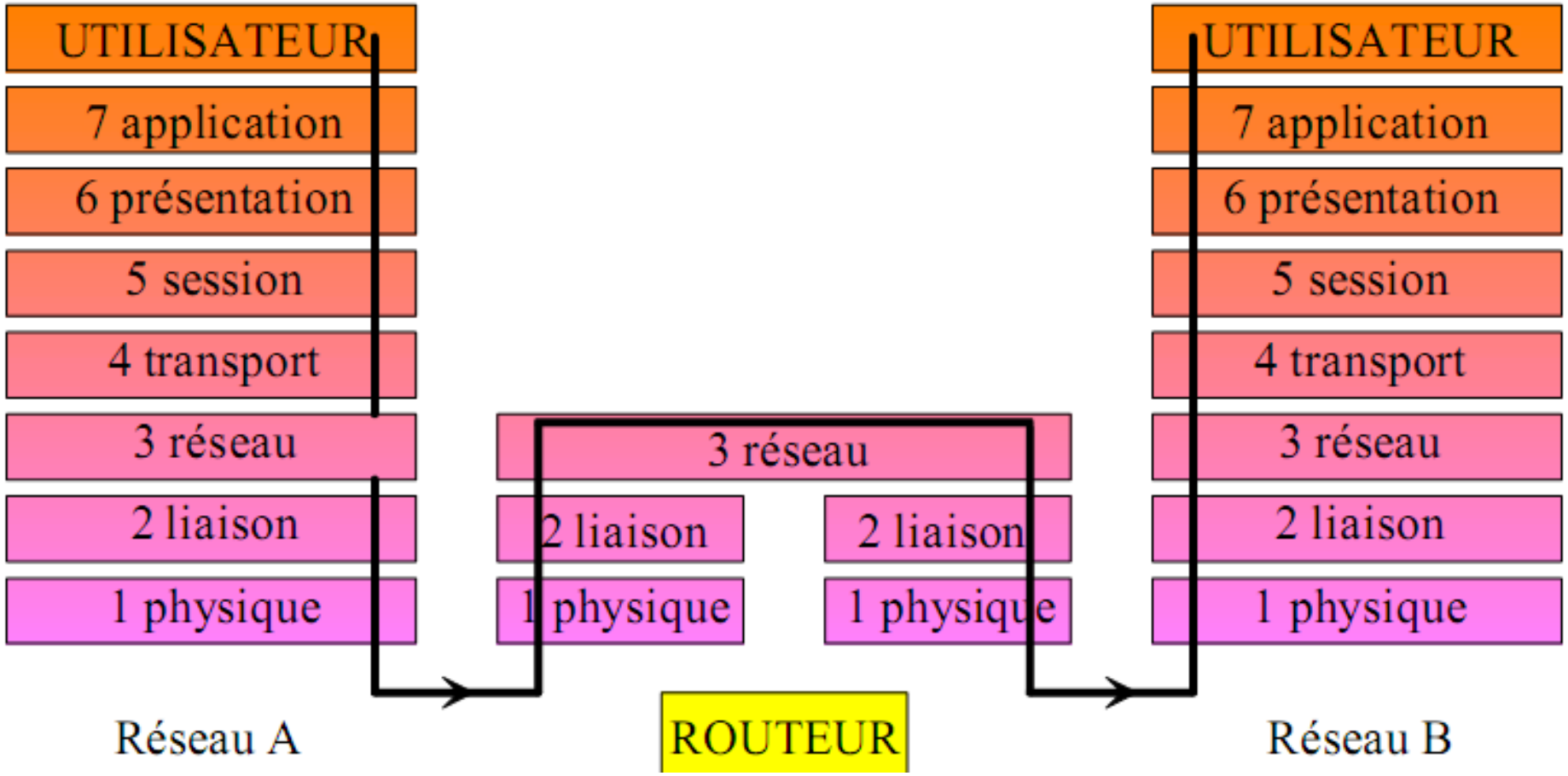
Qu’est ce qu’un routeur ?

- Equipement matériel et logiciel (de couche 3) qui fait en sorte que les paquets émis par une machine d’un réseau puissent atteindre une machine destinataire situé sur un réseau différent.
- Les paquets ne peuvent circuler entre réseaux différents que si ces réseaux sont reliés par un ou plusieurs routeurs.

Routeurs Cisco

Symbole d’un routeur

Le routeur et le modèle OSI



Rôle du routeur

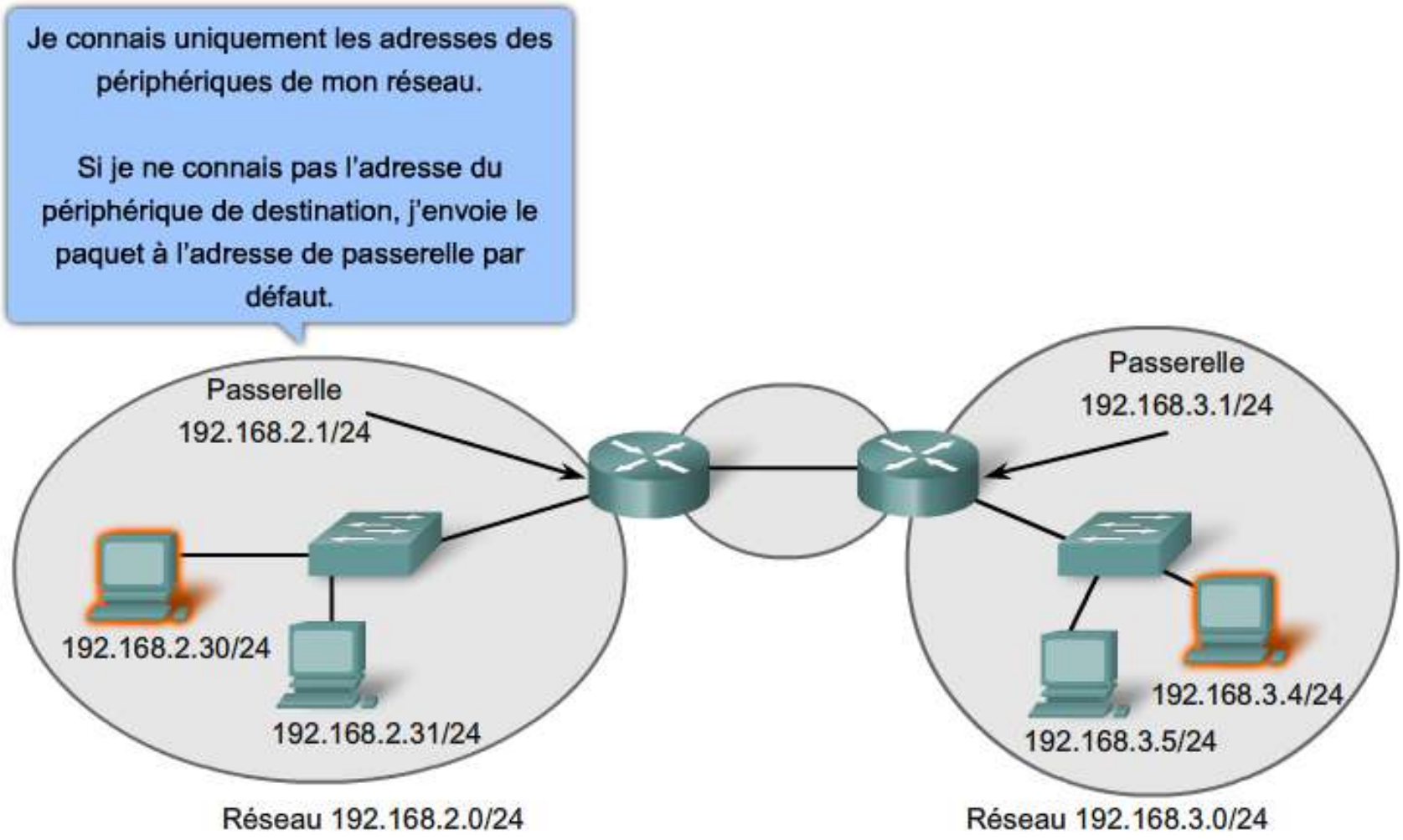
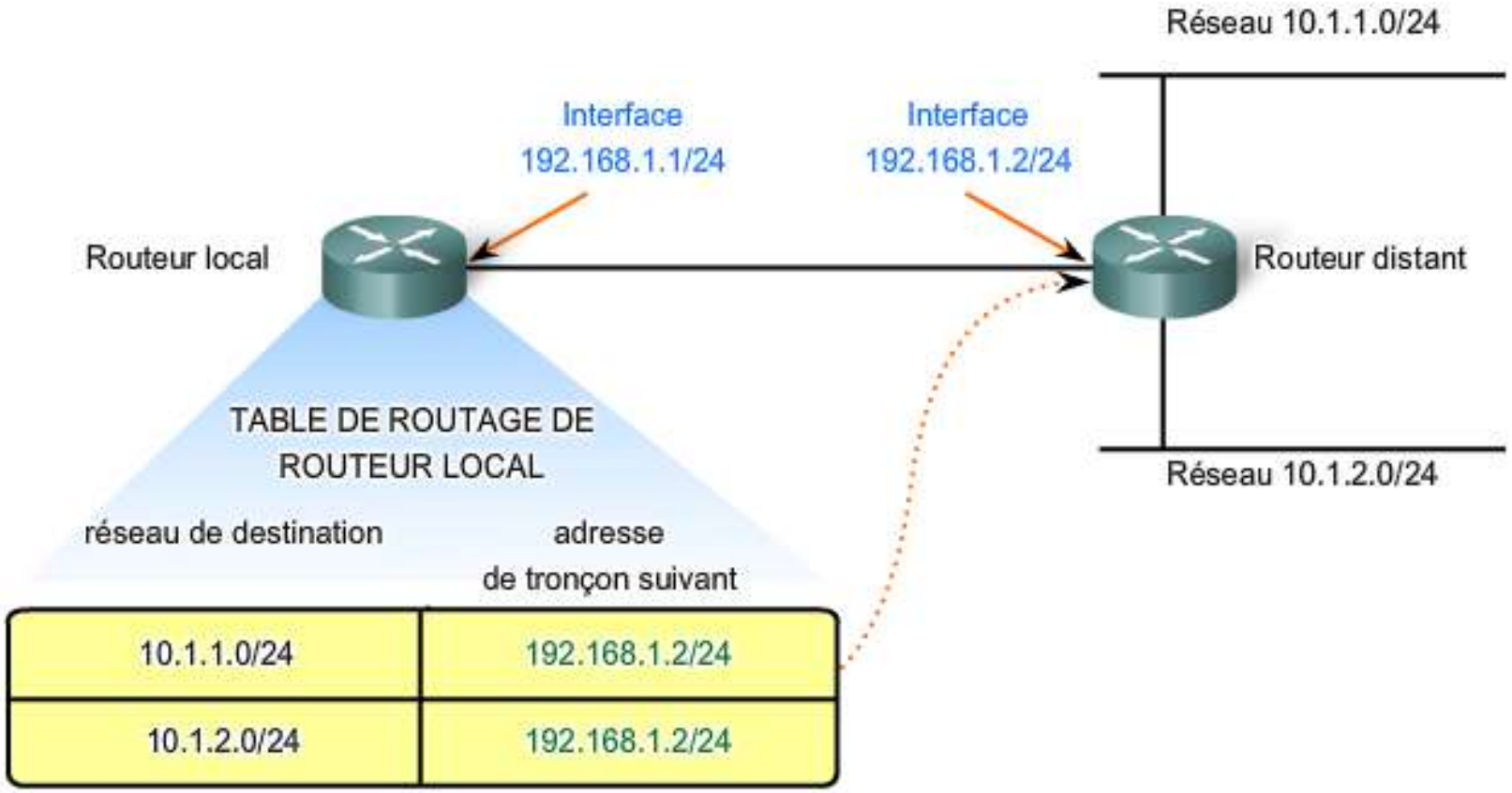


Table de routage

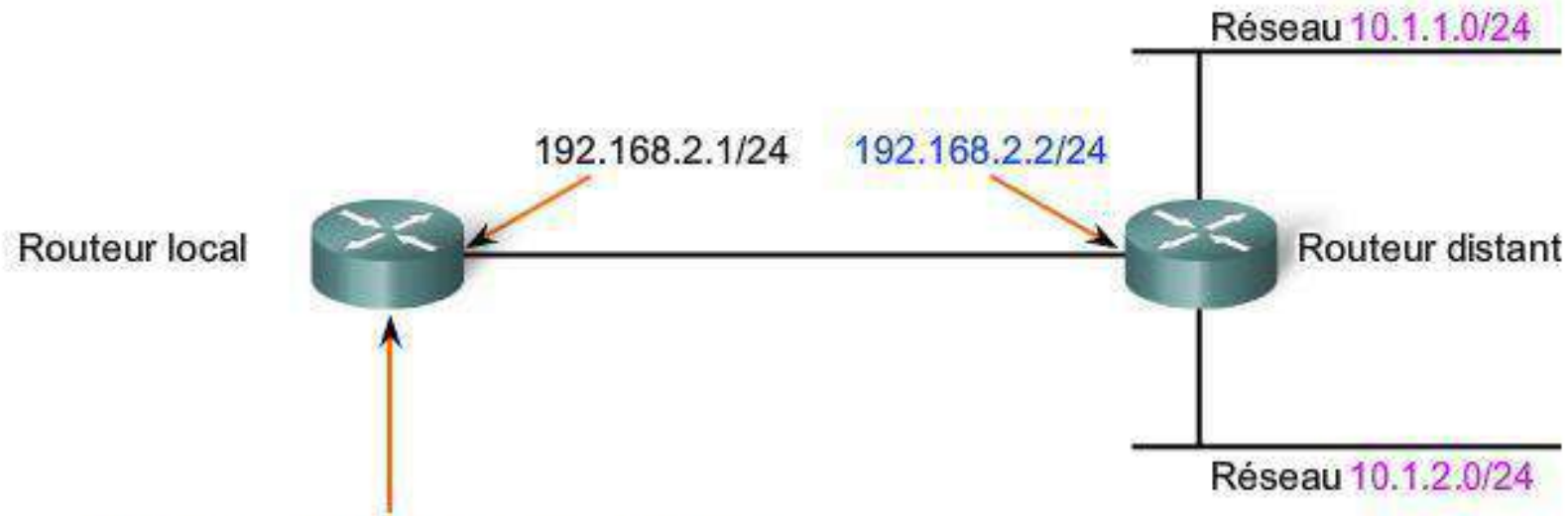


Le tronçon suivant pour les réseaux 10.1.1.0/24 et 10.1.2.0/24 à partir du routeur local est 192.168.1.2/24

Route par défaut

- Il s'agit d'une route qui correspond à tous les réseaux de destination.
- La route par défaut est utilisée pour diriger des paquets adressés aux réseaux qui ne sont pas explicitement mentionnés dans la table de routage.
- L'adresse **0.0.0.0** correspond à la route par défaut.

Exemple table de routage (Routeur CISCO)




```
   10.0.0.0/24 is subnetted, 2 subnets
R     10.1.1.0 [120/1] via 192.168.2.2, 00:00:08, FastEthernet0/0
R     10.1.2.0 [120/1] via 192.168.2.2, 00:00:08, FastEthernet0/0
C     192.168.2.0/24 is directly connected, FastEthernet0/0
S*    0.0.0.0/0 [1/0] via 192.168.2.2
```

Ceci est la sortie de table de routage du routeur local lorsque la commande show ip route est émise.

Routage IP : algorithme de base

- Extraire du paquet l'adresse IP de destination (**IPDest**).
- Calculer l'adresse du réseau de destination (**IPRes**) en appliquant un **AND** entre le **IPDest** et le **masque sous-réseau**.
- Si cette adresse IPRes correspond à l'adresse réseau du réseau local :
  - IPdest est directement accessible à partir du routeur.
  - Le routeur transmettra le paquet à la destination en utilisant le protocole ARP.

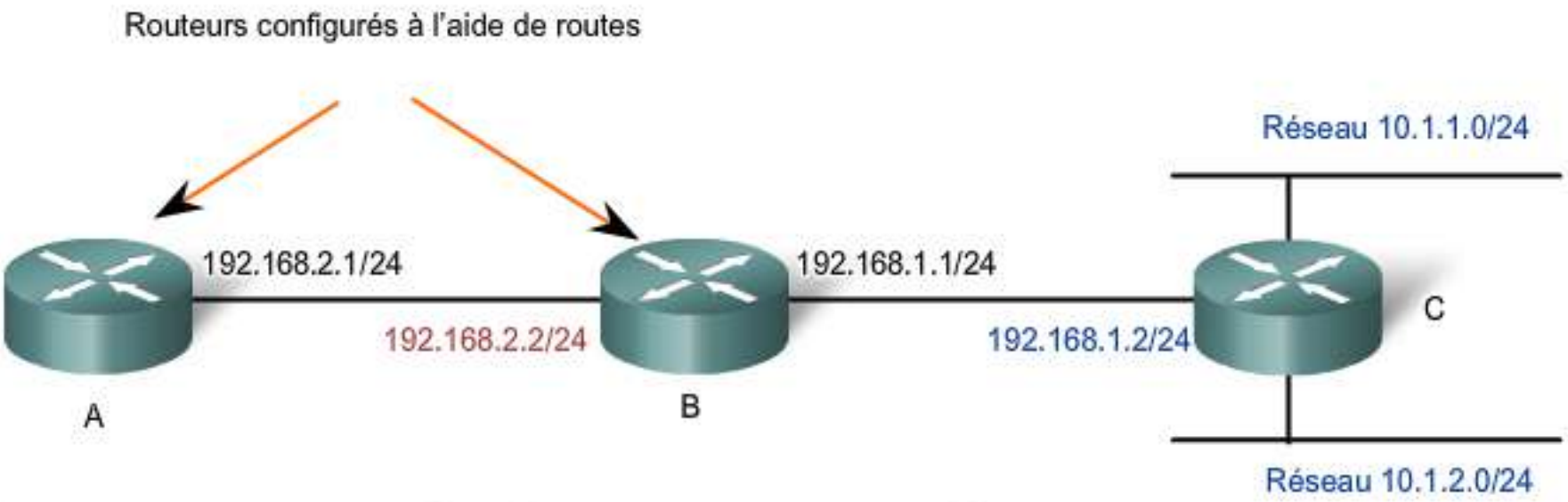
Routage IP : algorithme de base

- Sinon (ce n'est pas une adresse directement accessible, il faut alors consulter la table de routage IP locale) :
  - Si IPres est dans la table alors : Router le paquet selon les indications de la table.
  - Sinon IPres n'est pas dans la table alors : Prendre la route par défaut indiquée dans la table.
  - Si la route par défaut n'est pas configurée alors le paquet sera détruit.

Routage statique

- L’administrateur configure les routes de chaque routeur manuellement.
- Avantages :
  - Economie de la bande passante.
  - Sécurité.
- Inconvénients :
  - Configuration complexe pour les réseaux de grandes tailles.
  - Mise à jour difficile.

Routage statique



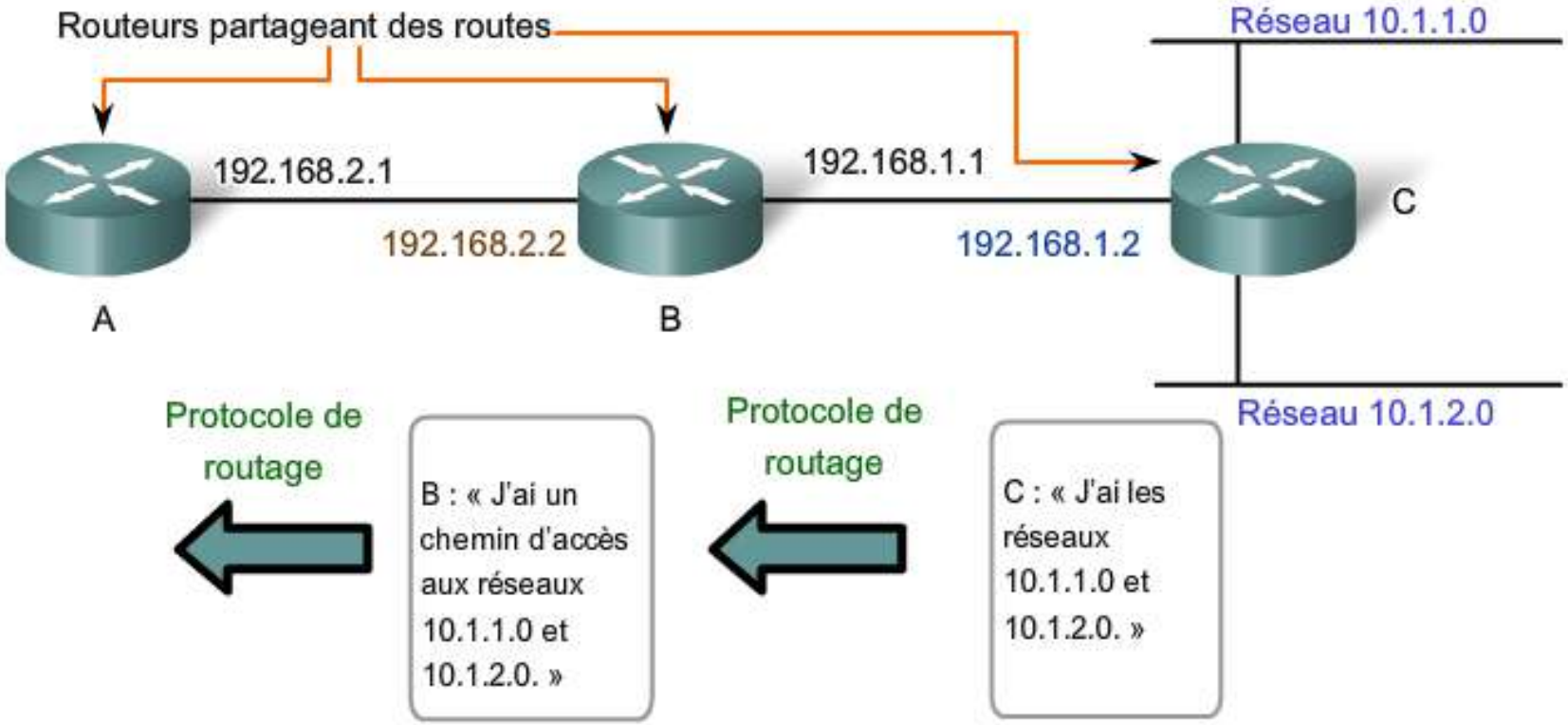
Routeur A:
192.168.2.2/24 configuré manuellement en guise de tronçon suivant pour les réseaux 10.1.1.0/24 et 10.1.2.0/24

Routeur B:
192.168.1.2/24 configuré manuellement en guise de tronçon suivant pour les réseaux 10.1.1.0/24 et 10.1.2.0/24

Routage dynamique

- La mise à jour des routes se fait d'une manière automatique.
- Un **protocole de routage** est utilisé afin de permettre aux routeurs de se comprendre et d'échanger des informations de façon périodique ou événementielle afin que chaque routeur soit au courant des évolutions du réseau sans intervention manuelle de l'administrateur du réseau.
- Avantages :
  - Mise à jour facile (automatique).
  - Meilleure performance.
- Inconvénients :
  - Consommation de la bande passante.
  - Vulnérable aux attaques.
  - Consommation supplémentaire des ressources physiques (CPU et RAM) des routeurs.

Routage dynamique



Le routeur B découvre de manière dynamique les réseaux du routeur C.

Le tronçon suivant du routeur B vers 10.1.1.0 et 10.1.2.0 est 192.168.1.2 (Routeur C).

Le routeur A découvre de manière dynamique les réseaux du routeur C à partir du routeur B.

Le tronçon suivant du routeur A vers 10.1.1.0 et 10.1.2.0 est 192.168.2.2 (Routeur B).

Différents types de protocoles de routage

- **Protocole de routage à vecteur de distance** : utilise un algorithme de routage qui additionne les distances pour trouver les meilleures routes (Algorithme Bellman-Ford). Souvent ils envoient l'entièreté de leur table de routage aux voisins. (Exemples : RIP et IGRP).
- **Protocole de routage à état de liens :** utilise un algorithme plus efficace (Dijkstra ou Shortest Path First). Les routeurs collectent l'ensemble des coûts des liens et construisent de leur point de vue l'arbre de tous les chemins. Les meilleures routes sont alors intégrées à la table de routage. (Exemples : OSPF et ISIS).
- **Un protocole de routage hybride** est un protocole de routage à vecteur de distance qui reprend des concepts d'états de liens. On citera EIGRP.

Réseaux informatiques

Chapitre 6 – Couche transport

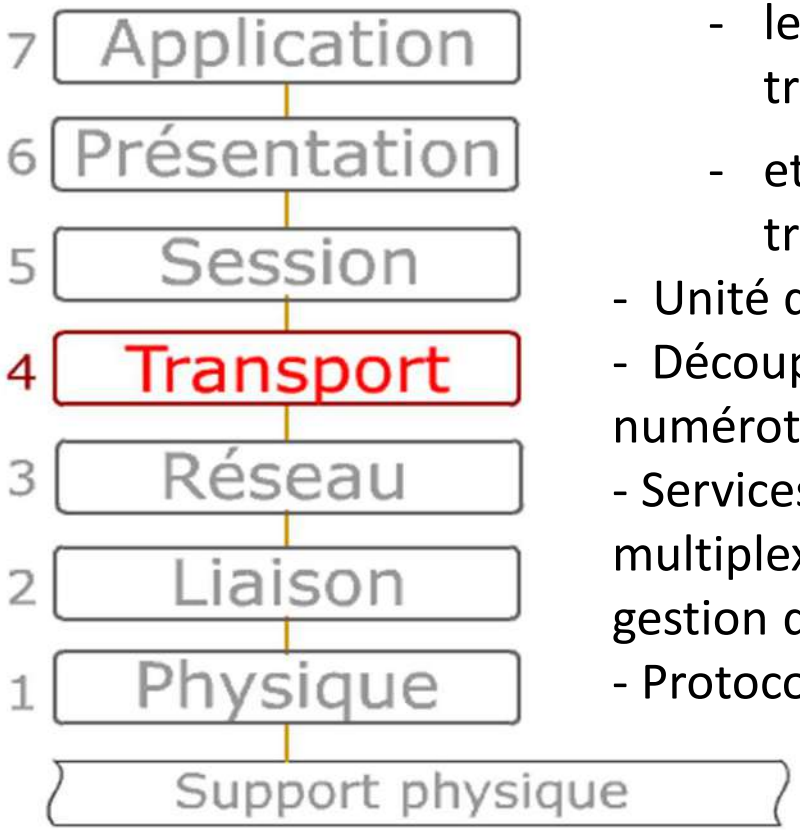
Mustapha Anwar BRAHAMI

ESSA Tlemcen

Références bibliographiques

- DORDOIGNE, J. (2015). Réseaux informatiques – Notions fondamentales (6ième édition). ENI. ISBN : 9782746093928
- LEGRAND, R. (2014). Notions de base sur les réseaux : 1er module de préparation à la certification CCNA 200-120. ENI. ISBN : 9782746092136
- DROMARD, D. (2006). Architecture des réseaux. Pearson. ISBN : 9782744076640
- LOHIER, S. (2010). Le réseau Internet : des services aux infrastructures. Dunod. ISBN : 9782100546046
- MEAOUA, A. Couche Transport TCP et UDP. UFR MI, Université Paris Descartes.
- SICARD, P. Couche Transport. Université Grenoble Alpes.
- DURIS, E (2010). Les couches transport TCP et UDP. Université Paris-Est Marne-la-Vallée.

Couche transport

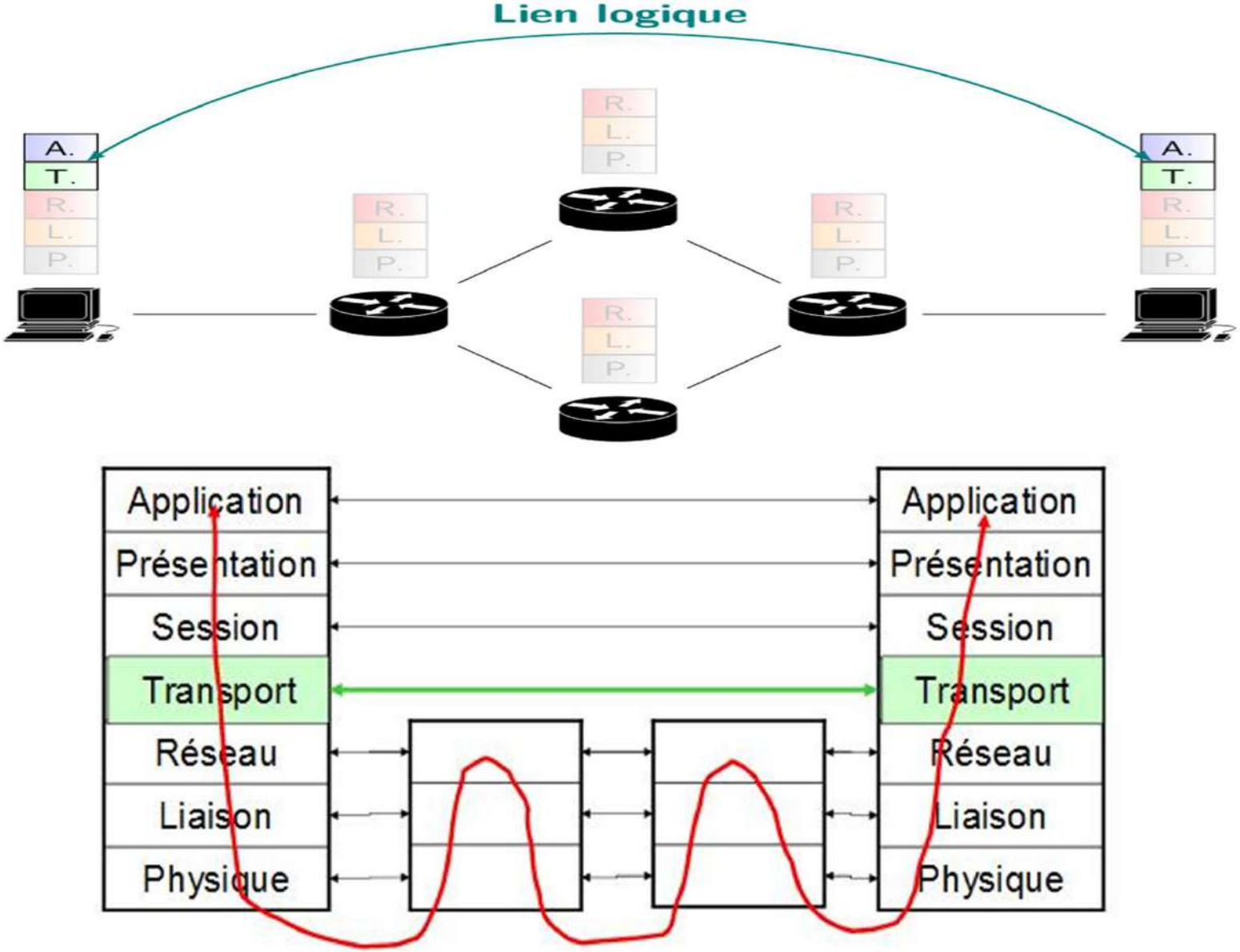


- Couche intermédiaire entre
  - les 3 couches supérieures orientées traitement
  - et les 3 couches inférieures orientées transmission
- Unité d'échanges : le segment.
- Découpe le message en segments qui seront numérotés.
- Services : segmentation, multiplexage/démultiplexage, contrôle de flux, gestion de la qualité de service (QoS)
- Protocoles : TCP, UDP …

Couche transport

- La couche transport est implémentée uniquement sur les équipements terminaux (n’est pas présente sur les éléments intermédiaires de type routeur), et assure la communication de bout en bout.

Couche transport



Couche réseau Vs. Couche transport

- La couche réseau assure la communication entre les hôtes, alors que la couche transport l'assure entre les applications.
- La couche réseau n'assure qu'un strict minimum de qualité de service, donc les besoins des applications doivent être couvert par la couche transport.
- Améliorer la fiabilité des transmissions de la couche réseau de l'émetteur au récepteur.

Multiplexage

- Le premier rôle de la couche transport est le multiplexage :
  - Pour chaque hôte, plusieurs applications en parallèle.
  - Mais les hôtes ont une seule adresse (IP), et l'on utilise donc une seconde valeur pour identifier le processus sur une machine : le numéro de port.
  - Une connexion (logique) est donc représentée par 4 valeurs : (Adresse source, port source) – (Adresse destination, port destination).

Démultiplexage

- L'opération de démultiplexage se fait au niveau de la destination :
  - Le destinataire reçoit les différents segments.
  - Chaque segment a un numéro de port source et un numéro de port de destination.
  - Le destinataire utilise le numéro de port de destination pour diriger le segment vers l'application appropriée.

UDP (User Datagram Protocol)

- Mode sans connexion
- Transport non fiable
- Envoi direct des informations
- Aucun contrôle de flux
- Pas de garantie de séquencement
- Détection d’erreur optionnelle
- Usage : Applications multimédias

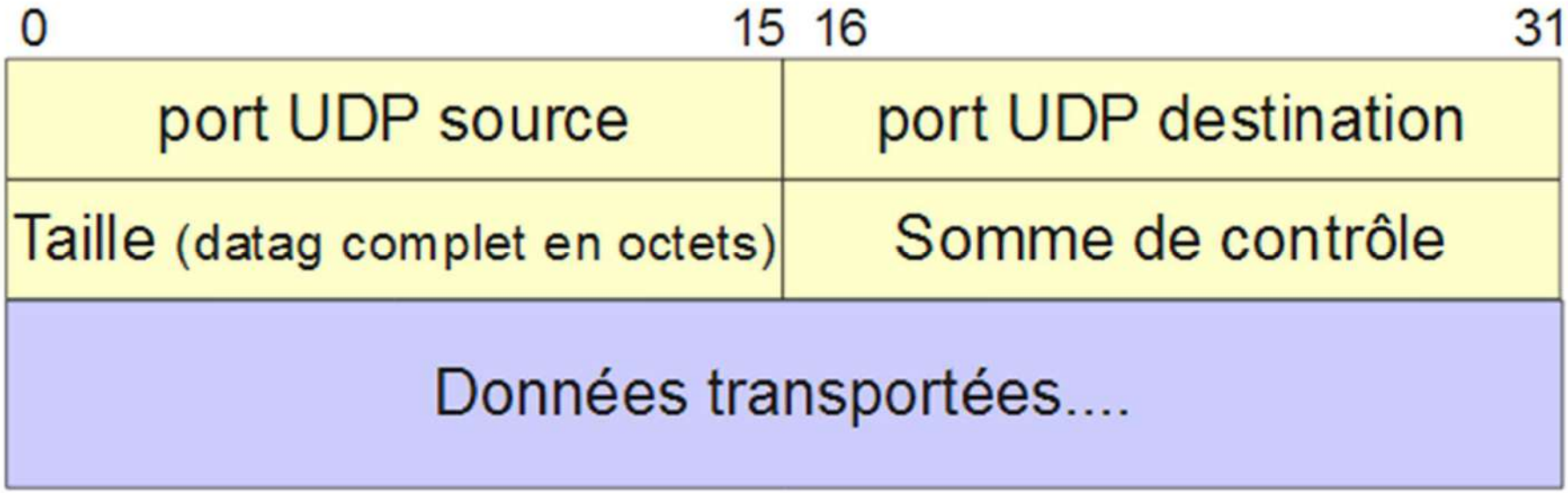
TCP (Transport Control Protocol)

- Service orienté connexion :
  - Phase de connexion / de transfert des données / déconnexion
- Garantie du séquencement :
  - Numérotation des segments
- Transport fiable :
  - Contrôle des erreurs + acquittements + retransmission
- Contrôle de flux
  - L'émetteur ne submerge pas le récepteur.
- Usage : Applications critiques

Caractéristiques UDP

- Avantages :
  - Protocole de transport le plus simple :
    - Échanges simples de messages courts client/serveur
      - DNS (Domain Name Service) :
        Question: « Quelle est l'adresse de google.fr?»
        Réponse: « google.fr est à 72.14.221.104»
  - Sans délai de connexion
  - Petit entête
- Inconvénients :
  - Manque de fiabilité (pas nécessaire pour les applications de vidéo diffusion ou de VoIP)
  - Aucune gestion de la congestion (les routeurs sont la seule solution pour réduire cet effet)
- Applications utilisant UDP : DNS, SNMP, DHCP, …

Format du segment UDP



UDP : les ports standards

No port	Mot-clé	Description
7	ECHO	Echo
11	USERS	Active Users
13	DAYTIME	Daytime
37	TIME	Time
42	NAMESERVER	Host Name Server
53	DOMAIN	Domain Name Server
67	BOOTPS	Boot protocol server
68	BOOTPC	Boot protocol client
69	TFTP	Trivial File transfert protocol
123	NTP	Network Time Protocol
161	SNMP	Simple Network Management prot.

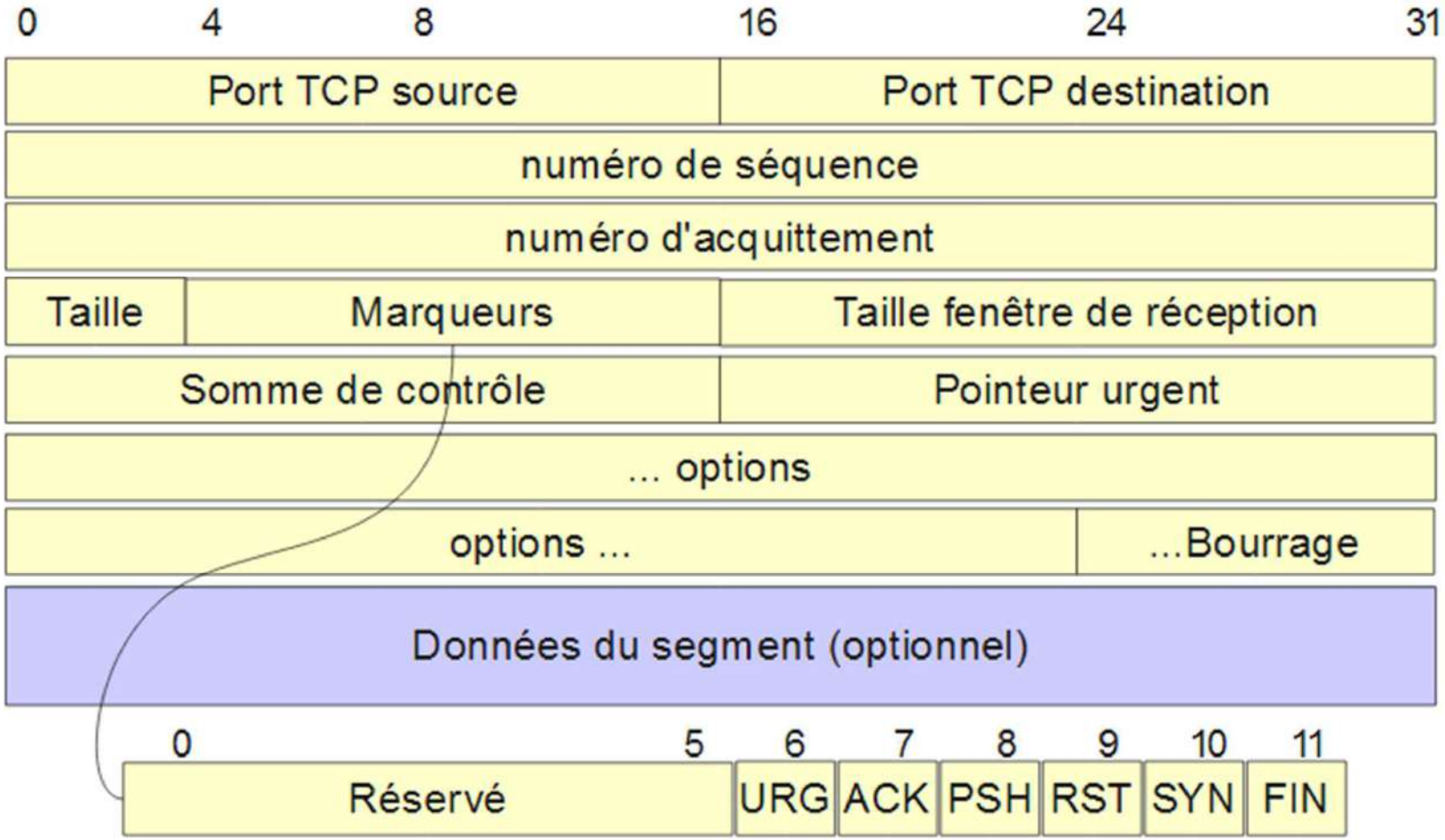
Caractéristiques TCP

- Communication :
  - Fiable : les données perdues par le réseau sont réémises.
  - Mode connecté : Phase de connexion / de transfert des données / déconnexion
- Contrôle de congestion
- Assez lourd à implanter (beaucoup plus qu'UDP)

Principe des segments TCP

- La **fiabilité** est obtenue par un mécanisme d'**acquittement** des segments :
  - À l'émission d'un segment, une alarme est amorcée.
  - Elle est désamorcée quand l'acquittement correspondant est reçu.
  - Si elle expire, le segment est réémis.
- Chaque segment possède un **numéro de séquence** :
  - Pour préserver l'ordre et éviter les doublons.
  - Les acquittements sont identifiés par un marqueur ACK.
  - Transport dans un même segment : les données et l'acquittement des données.

Format du segment TCP



Format du segment TCP

- Champ Taille : en nombre de mots de 32 bits
- Marqueurs :
  - URG : données urgentes
  - ACK : acquittement
  - PSH : force l'émission immédiate
  - RST : refus de connexion
  - SYN : synchronisation pour la connexion
  - FIN : terminaison de la connexion
- Somme de contrôle : utilisation de la vérification polynomiale (CRC)
- Options : taille max. de segment …

TCP : les ports standards

No port	Mot-clé	Description
20	FTP-DATA	File Transfer [Default Data]
21	FTP	File Transfer [Control]
23	TELNET	Telnet
25	SMTP	Simple Mail Transfer
37	TIME	Time
42	NAMESERVER	Host Name Server
43	NICNAME	Who Is
53	DOMAIN	Domain Name Server
79	FINGER	Finger
80	HTTP	WWW
110	POP3	Post Office Protocol - Version 3
111	SUNRPC	SUN Remote Procedure Call

Réseaux informatiques

Chapitre 6 – Couches session, présentation et application

Mustapha Anwar BRAHAMI

ESSA Tlemcen

Références bibliographiques

- DORDOIGNE, J. (2015). Réseaux informatiques – Notions fondamentales (6ième édition). ENI. ISBN : 9782746093928
- LEGRAND, R. (2014). Notions de base sur les réseaux : 1er module de préparation à la certification CCNA 200-120. ENI. ISBN : 9782746092136
- DROMARD, D. (2006). Architecture des réseaux. Pearson. ISBN : 9782744076640
- LOHIER, S. (2010). Le réseau Internet : des services aux infrastructures. Dunod. ISBN : 9782100546046
- FERRAND P (2013). Réseaux. INSA de Lyon. http://www.ferrand.cc/pdfs/cours_reseaux.pdf
- DUVALLET C (2016). Architecture et protocoles des réseaux. Université du Havre.

Couche session

Couche session

- Elle est chargée de l'ouverture, du maintien et de la fermeture d'une session entre applications.
- Elle est donc fortement liée aux notions suivantes :
  - Authentification : ouverture de session avec login/mot de passe.
  - Permissions : droits accordés à l'utilisateur pendant la session.

Couche présentation

Couche présentation

- Chargée du codage des données applicatives :
  - Les couches 1 à 5 ne se préoccupent pas de la signification des octets qu'elles transportent.
  - La couche 6 prépare ces données pour la couche application.
  - Exemple : Encodage de caractères (ASCII, UTF-8, ISO ...).
- La couche présentation peut aussi réaliser du cryptage ou de la compression.

Couche application

Couche application

- Dernière couche du modèle OSI.
- Elle est la source et la destination finale de toutes les données échangées entre les utilisateurs.
- C'est la couche qui fournit les interfaces pour la communication entre les utilisateurs.
- Les protocoles de la couche application tournent sur des équipements terminaux → n'est pas implémentée au niveau des équipements de cœur de réseau (équipements intermédiaires).

Classes d'applications

- Grand public : mail, web, messagerie instantanée, partage de fichier (P2P...), jeux en réseau, streaming vidéo, VoIP (téléphonie), transfert de fichiers, vidéoconférence.
- Informatique pour informaticiens : utilisation de terminal distant, système de fichier réparti, gestion de réseau.
- Spécialisées : bourse, industrie, santé, transport, nucléaire, spatiale, météo, calcul scientifique.

Architectures des applications

- Architecture client-serveur :
  - Le serveur est une application, hébergée par une machine hôte toujours allumée, avec un accès permanent et fixe.
  - Le client communique avec le serveur de manière intermittente.
  - Les clients ne communiquent pas directement entre eux, mais passent par le serveur.
  - Exemple : navigateur – serveur web.
- Pair à pair (Peer-2-Peer (P2P)) :
  - Pas de serveur.
  - Les équipements terminaux communiquent entre eux directement, et s'échangent un service.
  - Performances intéressantes, mais gestion compliquée car les équipements changent constamment.
  - Exemple : torrent.

HTTP : HyperText Transfer Protocol

- Utilisation de la notion d'hypertexte, où un document contient des liens vers d'autres objets ou documents.
- Une page web est formée d'un fichier écrit en langage HTML (Hypertext Markup Language), qui référence plusieurs objets.
- Chaque page web est identifiée par une URL (Universal Resource Locator) :

http://www.essa-tlemcen.dz/emploi-du-temps.html

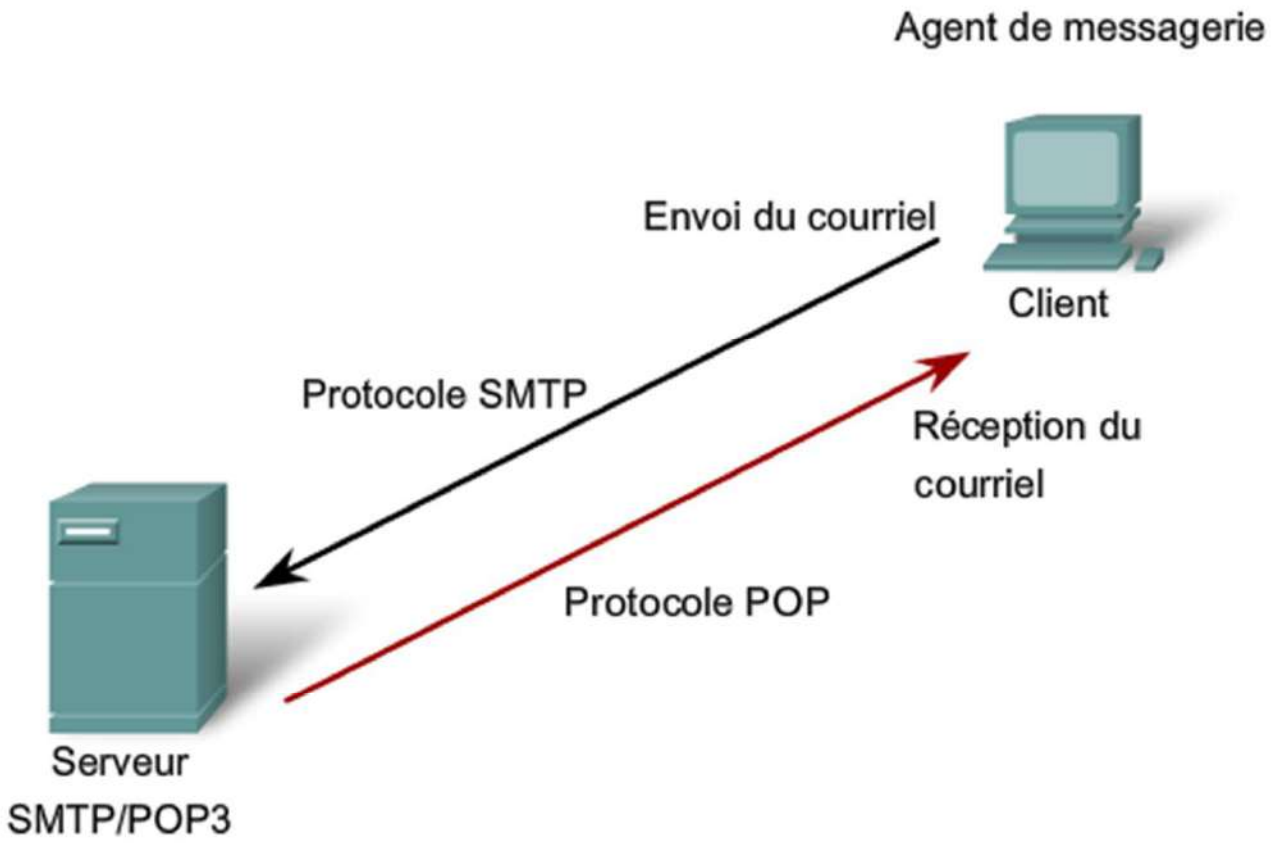
Nom du serveur — Nom de la page Web

- Les objets (fichiers) sont stockés sur un serveur HTTP (appelé couramment serveur Web).
- Même si d'autres langages sont utilisés pour gérer l'application sur le serveur (PHP : pages dynamiques, …), les pages et la syntaxe suivent les standards HTML et HTTP.
- HTTP fonctionne sur TCP et utilise le port 80.

Le courrier électronique

- L'application la plus répandue dans les réseau, par sa simplicité et sa vitesse d'exécution, a révolutionné la manière dont nous communiquons.
- Utilisation d'un client de messagerie qui fournit les fonctionnalités de deux protocoles SMTP et POP :
  - SMTP : pour envoyer les courriels au serveur mail (port TCP numéro 25).
  - POP : pour recevoir le courriel à partir du serveur mail (port TCP numéro 110).

Le courrier électronique



Les clients envoient des courriels à un serveur via le protocole SMTP et en reçoivent via le protocole POP3.

FTP : File Transfer Protocole

- Utiliser pour le transfert/téléchargement des fichiers.
- 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.
- FTP fonctionne sur TCP et utilise le port 21 pour les commandes, et le port 20 pour les données.

Telnet : ***Te**rminal **net**work*

- Telnet : est un utilitaire de prise de commandes à distance qui offre un éventail de fonctionnalités permettant l'exécution interactive de commandes dans l'environnement distant.
- Une connexion Telnet se fait en deux phases :
  - une phase d'authentification.
  - une phase de travail à distance.
- Fonctionne en mode connecté (TCP) sur le port 23.

DHCP : Dynamic Host Configuration Protocol

- DHCP : Attribuer automatiquement une adresse IP à une machine qui se connecte au réseau.
- Permet de faciliter la gestion des adresses de machines dans les réseaux de grandes tailles qui se modifient souvent.
- L'attribution se fait sur plusieurs phases :
  1. Le client envoie un paquet d'exploration DHCPDISCOVER en broadcast en utilisant l'adresse 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 fonctionne sur UDP et utilise le port 67.

DNS : Domain Name System

- Permet d'associer des noms symboliques (facile à retenir) à des adresses numériques, en général des adresses IP.
- 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).