Fiche de RES101

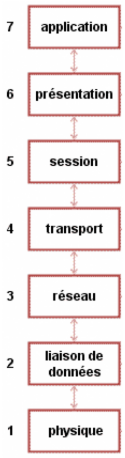
Notions utiles

- **Réseau** : infrastructure et ensemble des mécanismes permettant à plusieurs entité réparties de communiquer avec la meilleure performance possible.
- Exemples de réseaux :
  - Réseau téléphonique commuté (RTC) : réseau dédié, téléphonie classique.
  - Réseaux cellulaires (GSM)
  - Réseaux locaux (LAN) : quelques dizaines de terminaux.
  - Réseau étendu (WAN) : opéré par un service de télécommunications.
- **Débit** d'un flux : volume de données émis par unité de temps.
- **Capacité** d'un réseau : quantité d'informations qu'il peut acheminer par unité de temps ; peut ralentir un débit ou conduire à des pertes de données.
- **Latence** : temps de propagation d'une unité de donnée entre un émetteur et un récepteur.
- **Gigue** : variation du délai de transmission → arythmie des flux → mise en place de tampons (buffers) à la réception.
- **Broadcast** : type de paquet envoyé à tout le monde.
- *Network Interface Card* (NIC) : fournit la connexion physique entre le réseau et un terminal.

Modèle OSI

Def : le modèle OSI est né quand nous avons commencé à avoir une certaine expérience des communications entre ordinateurs. Son objectif est de normaliser les communications pour garantir un maximum d'évolutivité et d'interopérabilité entre les ordinateurs.

— Le modèle OSI est un modèle en couches. Cela veut dire qu'il est découpé en plusieurs morceaux appelés couches.



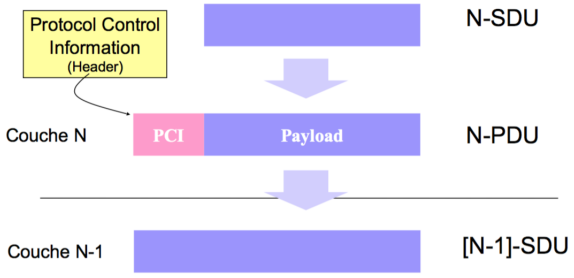
— Couche 1 : **physique** (câbles,...) → offrir un support de transmission pour la communication.
— Couche 2 : **liaison** (lien direct, point à point) → connecter les machines entre elles sur un réseau local (+ détecter les erreurs et fiabiliser la connexion physique entre deux réseaux) → adresses MAC, *Switch*.
— Couche 3 : **réseau** → interconnecter les réseaux entre eux, càd trouver un chemin pour envoyer des données d'un terminal à un autre à travers un réseau hétérogène et fragmenter les paquets → *routeur*.
— Couche 4 : **transport** → gérer les connexions applicatives et garantir la connexion → TCP / UDP, ports, différentiation des services.
— Couche 5 : **session** (rarement implémentée).
— Couche 6 : **présentation** → définit une syntaxe commune pour la représentation des données.
— Couche 7 : **application** → source et destination des données à transporter.

Deux règles pour les couches :

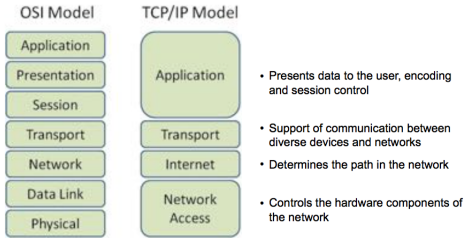
— Chaque couche est indépendante (ex : adressage IP (couche 3) interchangeable (IPv4 ↔ IPv6) sans toucher aux autres couches).
— Chaque couche ne peut communiquer qu'avec une couche adjacente. (Envoi de données : de haut en bas ≠ Réception de données : de bas en haut).

Principe de l'architecture des couches :

— Les unités de données échangées : **SDU**.
— Les unités de données manipulées **PDU** (= SDU + **PCI** (champs spécifique au control du protocole)).



TCP/IP vs OSI Model :



Réseaux locaux : couche liaison de données (PHY/MAC)

Problématique de l'accès partagé : il peut être intéressant de partager un même support physique/logique entre plusieurs terminaux.

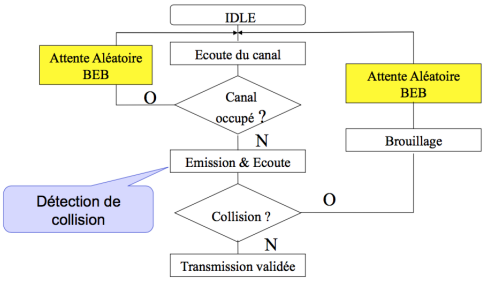
— Il existe deux type de transmission : asynchrone (peut débuter à n'importe quel instant) et synchrone (on divise le temps en intervalles T et la transmission ne peut débuter qu'en début de slot).
— Il est existe deux types de stratégies : déterministe (qui évite les collisions en partageant les bandes) et aléatoire qui ne peuvent pas éviter les collisions.

Protocole ALOHA/ALOHA discrétisé

— **Principe ALOHA :** N stations envoient des données à une station centrale, une station est autorisée à émettre dès qu'elle a un paquet à envoyer.
— Émission sur la fréquence f_1 dès qu'elle a un paquet.
— Risque de perte de paquet si collision ou bruit du canal trop élevé.
— Si au bout d'un aller retour l'utilisateur ne reçoit pas d'acquittement, il ré-emet son paquet au bout d'un délai aléatoire.
— **Principe ALOHA discrétisé :** le temps est divisé en intervalles de temps égaux. Une station spéciale est chargée d'émettre un signal permettant la synchronisation des stations.
— **Critère de performance :** Débit normalisé (proportion du temps pendant lequel le canal est utilisé), Délai, Stabilité, Équité entre les stations.

CSMA/CSMA-CD : Protocoles à détection de porteuse : les stations adapent leur comportement à l'activité du canal (si occupé, il ne faut pas émettre, et s'il est libre on transmet). Plusieurs types :

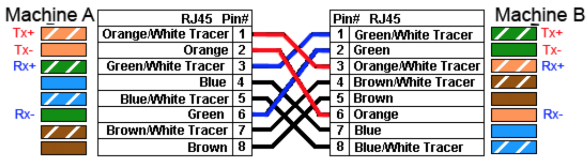
— CSMA 1-persistant : Lorsque le canal est libre, l'émission se fait avec une probabilité 1 $\longrightarrow$ proba de collision élevé si le trafic est important.
— CSMA non persistant : si canal occupé on introduit une attente aléatoire en plus $\longrightarrow$ probabilité de collision réduite.
— CSMA p-persistent : si le canal n'est pas occupé on émet avec une probabilité p (plus le nombre de stations est important, plus faible doit être p et donc plus important est le délai).
— CSMA-CD : on peut émettre et sonder le signal simultanément, lorsqu'une collision est détectée, la transmission en cours est interrompu + Choix de la période d'attente (Binary Exponential Backoff BEB) : Après i collision on attend de façon aléatoire entre 0 et $2^i - 1$.



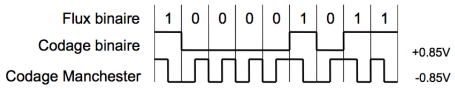
— Paramètre $a = \tau/T$ le rapport période de vulnérabilité sur temps de propagation maximal. a est lié aux protocoles CSMA.

Ethernet

— Protocole de réseau local à commutation de paquets.
— Généralement des câbles croisées torsadés à 8 fils (on utilise couramment 4 fils, deux à l'émission et deux à la transmission).
— La sortie est en général en RJ45.

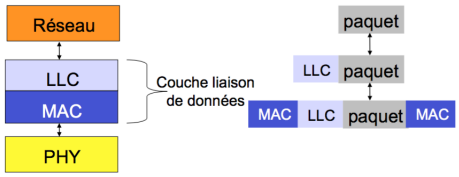


— Deux types de codage : codage en bande de base (narmol) et le codage de Manchester :



Couches MAC

— L'adresse MAC est universelle : une station s'attachant à un réseau est sur d'avoir une adresse unique.
— Les 24 premiers bits sont assignés au constructeur par l'IEEE, les 24 derniers sont sont choisis par le constructeur de la carte
— l'adresse broadcast : `ff:ff:ff:ff:ff:ff`
— *Contrôle de liaison logique (LLC)* : fiabilise une communication point à point (gestion des erreurs et controle de flux). Offre 3 types de service à une couche réseau $\longrightarrow$ mode sans connexion non-acquitté, mode orienté connexion, mode sans connexion avec acquittements.



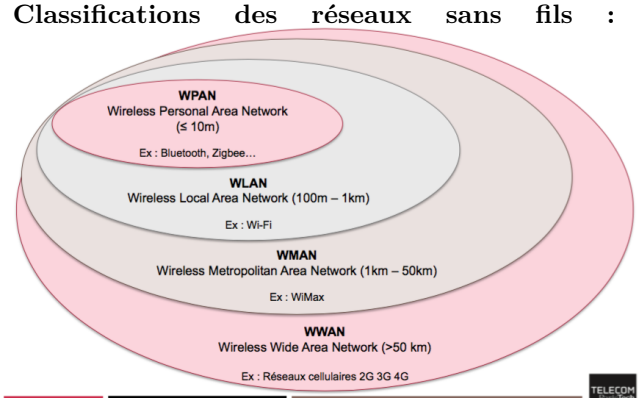
Interconnexion des réseau locaux

— Réparateur : décode les données et les transmet sur tous les segments auxquels il est attaché.
— Concentrateur (hub) : topologie en étoile, connecte, des brins entre eux et diffuse sur toutes les branches de l'étoile, équipement de niveau 1 $\sim$ multiprise réseau.
— Pont (bridge) : relie plusieurs réseaux de façon qu'ils constituent un seul réseau logique ; possède une adresse MAC et filtre les trames (laisse passer les trames de broadcast).
— Passerelle applicative : capable de travailler au niveau de toutes les couches ; peut décoder le format et le contenu et opérer des conversions.
— Passerelle de transport : connecte deux réseaux avec des couches de transport différentes.
— *Spanning tree protocol* : Suppression des boucles dans des topologies de réseau contentant des chemins redondants (on ne garde qu'un seul chemin en bloquant l'accès aux autres). On construit un graphe non orienté et connecté et calcule le plus court chemin à la racine (fondé sur l'adresse MAC + priorité).
— Les commutateurs (switch) : équipement "intelli-

gent” → possède une table avec les adresses MAC pour retransmettre les messages uniquement à la partie où se trouve le destinataire ; 4 à 32 cartes comprenant chacune 8 ports.
— Les apports sur switch : plus de CSMA/CD, il n'y a plus de collision avec les switch, la carte réseau fonctionne en **full duplex**.

Réseau sans fil

Classifications des réseaux sans fils :



Propagation radio :

$$P_r = P_e G_e G_r \left(\frac{K\lambda^2}{r^\alpha}\right) a_{\text{shadowing}} a_{\text{fading}}$$

avec :
— α : le coefficient d'atténuation (entre le vide et l'urbain)
— $a_{\text{shadowing}}$: effet de masque (objet entre émetteur et récepteur)
— a_{fading} : évanouissements rapide (variations raides du canal)

Wi-Fi - 2 bandes :
— Entre 2.4 et 2.48 GHz (avec 13 canaux en Europe)
— Entre 5.15 et 5.35 GHz : pour les radars météo et les usages militaires.
— **CSMA/CA** : On écoute avant d'émettre. Quand le médium est libre, on attend un délai fixe avant d'émettre.

Network (IP) Layer

Couche 3 : Interconnexion des réseaux (les couches 1 et 2 formaient les réseaux locaux, la couche 3 relie tout ces réseaux).

Adresse IP
— Codée sur 32 bits (de `0.0.0.0` à `255.255.255.255`)
— On ajoute une information supplémentaire à l'adresse IP qui est le masque de sous-réseau (ces deux parties sont inséparable)
— Le masque indique quelle est la partie réseau de l'adresse, et quelle est la partie machine. Les 1 représente la partie réseau, et les 0 la partie machine
— Exemple : `255.255.0.0` ⟶ `11111111.11111111.000000000.00000000`
`192.168.0.1` ⟶ `11000000.10101000.000000000.00000001`

Calcul de la première et de la dernière adresse d'un réseau
— On passe en binaire et on garde la partie de l'adresse qui correspond à la partie réseau, la première adresse est la partie machine avec que des 0 et la dernière est la partie machine avec des 1.
— La première et la dernière adresse ne sont pas utilisable pour une machine. La première adresse est l'adresse du réseau et la deuxième représente l'adresse de broadcast.

Les différentes classes d'adresse IP :
— **Classe A :** Le premier octet a une valeur comprise entre 1 et 126 ; soit un bit de poids fort égal à 0. Ce premier octet désigne le numéro de réseau et les 3 autres correspondent à l'adresse de l'hôte ⟶ de `1.xxx.xxx.xxx` à `126.xxx.xxx.xxx`
— **Classe B :** Le premier octet a une valeur comprise entre 128 et 191 ; soit 2 bits de poids fort égaux à 10. Les 2 premiers octets désignent le numéro de réseau et les 2 autres correspondent à l'adresse de l'hôte ⟶ de `128.0.xxx.xxx` à `191.255.xxx.xxx`
— **Classe C :** Le premier octet a une valeur comprise entre 192 et 223 ; soit 3 bits de poids fort égaux à 110. Les 3 premiers octets désignent le numéro de réseau et le dernier correspond à l'adresse de l'hôte ⟶ de `192.0.0.xxx` à `223.255.255.xxx`
— **Classe D :** Le premier octet a une valeur comprise entre 224 et 239 ; soit 3 bits de poids fort égux à 111. Il s'agit d'une zone d'adresses dédiées aux services de multidiffusion vers des groupes d'hôtes (host groups) ⟶ de `224.xxx.xxx.xxx` à `239.xxx.xxx.xxx`
— **Classe E :** Le premier octet a une valeur comprise entre 240 et 255. Il s'agit d'une zone d'adresses réservées aux expérimentations. Ces adresses ne doivent pas être utilisées pour adresser des hôtes ou des groupes d'hôtes ⟶ de `240.xxx.xxx.xxx` à `255.xxx.xxx.xxx`

Classe	Masque réseau	Adresses réseau	Nombre de réseaux
A	255.0.0.0	1.0.0.0 - 126.255.255.255	126
B	255.255.0.0	128.0.0.0 - 191.255.255.255	16384
C	255.255.255.0	192.0.0.0 - 223.255.255.255	2097152
D	240.0.0.0	224.0.0.0 - 239.255.255.255	adresses uniques
E	non défini	240.0.0.0 - 255.255.255.255	adresses uniques

Le routage : Le routeur est un matériel de couche 3 qui relie plusieurs réseaux.

- Quand le routeur reçoit la trame, il vérifie qu'adresse MAC est bien la bonne, et ensuite il utilise la table de routage qui va donc lister les routeurs auxquels je peux envoyer mon datagramme pour joindre une destination donnée.
- Fonctionne sur les adresses IP.
- La table de routage contient des adresses et des masques → la liste des réseaux que l'on peut joindre et les passerelles par lesquelles je dois passer pour les joindre. C'est une table de correspondance qui indique qui est le routeur suivant. Construire une table de routage se fait en 3 étapes :
  — indiquer les réseaux auxquels ma machine est

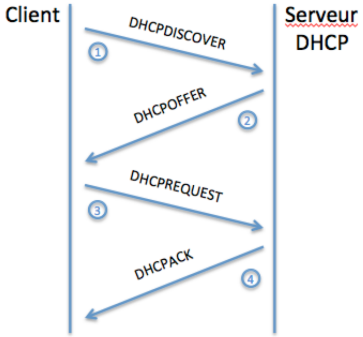
connectée ;
- indiquer la route par défaut ;
- indiquer tous les autres réseaux que je ne peux pas encore joindre avec les deux étapes précédentes.

Le protocole ARP : On veut connaître le chemin pour envoyer un message à une machine, sauf que l'on a pas son adresse MAC, il existe un protocole pour remédier à cela : ARP.

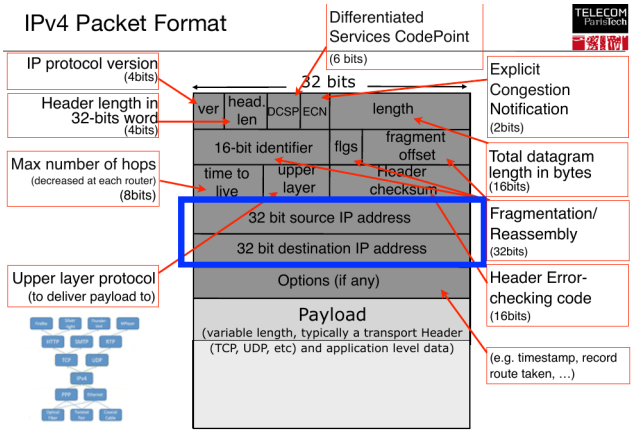
- On envoie un message de *broadcast*, en demandant à la personne dont on connait l'adresse IP de nous envoyer son adresse MAC : c'est la requête ARP.
- Sauf que si on envoie une requête à chaque fois que l'on veut transmettre un message on risque de saturer le réseau, d'où la **table ARP**.
- la table ARP garde en mémoire provisoirement les relation `adresse MAC` ↔ `adresse IP`, la table est dynamique, elle la garde en mémoire environ 2 minutes.

Le serveur DHCP : On se rend donc bien compte qu'il serait bien d'avoir un mécanisme rapide et fiable pour adresser les machines d'un réseau. C'est là qu'entre en jeu le protocole DHCP.

- La première fonction d'un serveur DHCP est de fournir des adresses IP aux machines en faisant la demande.
- Demande en *broadcast* en passant par l'adresse MAC : `ff:ff:ff:ff:ff:ff`



ICMP : ICMP est un protocole dans la suite protocolaire TCP-IP utilisé pour envoyer des messages d'erreurs dans un réseau. Il travaille en partenariat avec le protocole IP. Nous allons le voir en détail, voir les différents types d'erreurs, leurs codes, leurs significations et les scénarios dans lesquels elles se manifestent.



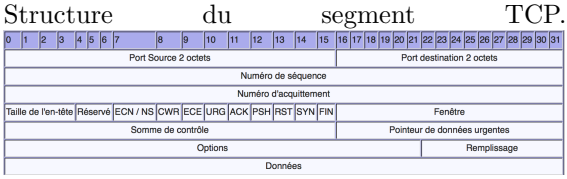
Couche de transport

Deux principaux protocoles de transport : **TCP** et **UDP**. UDP : User Datagram Protocol .

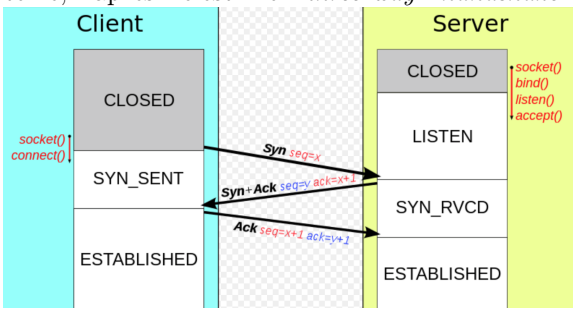
- Très simple, aucune garantie que les messages arrivent ou arrivent dans l'ordre, mais les performances sont élevé (utilisé par exemple pour skype, le streaming,...).
- Utilisé beaucoup en téléphone IP et en DHCP.

TCP : Transmission Control Protocol.

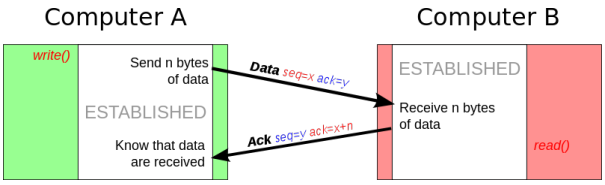
- En 3 étapes : établissement de la connexion, transfert de données et fin de la connexion.
- Pendant la phase d'établissement de la connexion, des paramètres comme le numéro de séquence sont initialisés afin d'assurer une transmission fiable (sans perte et dans l'ordre) des données.
- Structure du segment TCP.



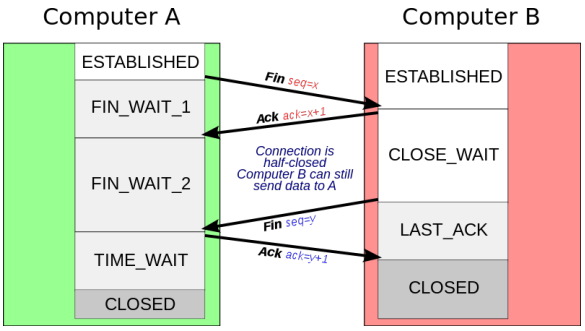
- **Établissement d'une connexion :** un système ouvre une *socket* et attend une demande de connexion d'un autre système, après c'est le *three-way handshake*.



- **Transfert de données :** certains mécanismes clés permettent d'assurer la robustesse et la fiabilité de TCP. En particulier, les numéros de séquence sont utilisés afin d'ordonner les segments TCP reçus et de détecter les données perdues, les sommes de contrôle permettent la détection d'erreurs, et les acquittements ainsi que les temporisations permettent la détection des segments perdus ou retardés.

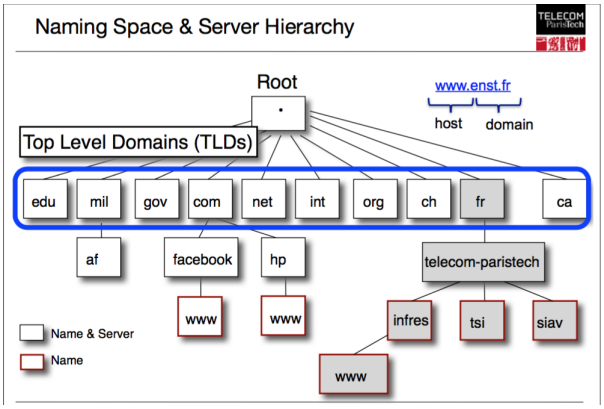


— **Terminaison d'une connexion :** la phase de terminaison d'une connexion utilise un *handshaking* en quatre temps, chaque extrémité de la connexion effectuant sa terminaison de manière indépendante. Ainsi, la fin d'une connexion nécessite une paire de segments FIN et ACK pour chaque extrémité.



— **Contrôle de flux :** chaque partenaire dans une connexion TCP dispose d'un tampon de réception dont la taille n'est pas illimitée. Afin d'éviter qu'un hôte ne surcharge l'autre, TCP prévoit plusieurs mécanismes de contrôle de flux. Ainsi, chaque segment TCP contient la taille disponible dans le tampon de réception de l'hôte qui l'a envoyé. En réponse, l'hôte distant va limiter la taille de la fenêtre d'envoi afin de ne pas le surcharger.

— **Contrôle de congestion :** la congestion intervient lorsque trop de sources tentent d'envoyer trop de données trop vite pour que le réseau soit capable de les transmettre. Ceci entraîne la perte de nombreux paquets et de longs délais. Les émetteurs et destinataires TCP peuvent modifier le comportement du flux de données.



— Le système de noms de domaine est géré par un organisme américain appelé l'ICANN. L'ICANN est responsable de la gestion des 13 serveurs DNS qui gèrent la racine du DNS. Ces 13 serveurs connaissent les adresses IP des serveurs DNS gérant les TLD (les .fr, .com, org, etc...).

QoS et QoE

Qualité de service (network-centric)

— bande-passante,
— probabilité de perte (paquet arrivé avec trop d'erreur ou perdu à une file d'attente),
— délai,
— gigue.

Qualité d'expérience (user-centric)

— orienté données : temps de complètement, fiabilité,...
— multimédia : *Mean Opinion Score*, *Perceptual Evaluation of Video Quality*,...

Le service DNS

Domain Name System ← indispensable au fonctionnement d'internet. Un nom de domaine se décompose en plusieurs parties.

— l'extension en premier : on parle de Top Level Domain. Il existe des TLD nationaux (fr, it, de, es, etc.) et les TLD génériques (com, org, net, biz, etc...).