Cours **Réseaux**

# Fiche de Rapport

**INFORMATIONS ETUDIANT :**

**PRENOM : SOULEYMANE**

## NOM : DIALLO

**EMAIL :** diallo.souleymane1@uam.edu.sn

## Concepts Généraux :

* **Etudier un réseau** : c’est étudier les équipements et les logiciels
* Les équipements à étudier :
  + Les cartes réseaux
    - Les cartes réseau sans fil
    - Les cartes réseaux filaires
  + Les switches ou commutateurs permettant d’interconnecter les machines
  + Les routeurs qui sont des équipements permettant d’orienter les données à travers un réseau.
* Logiciels à étudier :
  + Les systèmes d’exploitation Windows, Linux, Mac OS
  + Les systèmes d’exploitation des équipements tel que Cisco, Juniper, Huawei, etc.
* **Les couches protocolaires** : donnent des règles de communication entre deux couches
* **GNS3** : logiciel permettant d’émuler des équipements tels que PC, switch, routeurs et firewall
* **Virtual Box** : un logiciel permettant de créer et gérer les machines virtuelles
* **Wireshark** : logiciel permettant d’analyser des données réseaux et de voir leur composition
* **NodeJs :**  permet de développer des applications aussi bien coté frontend que backend
* **PORT CONSOLE** : utilisé pour paramétrer un routeur ou un switch
* **Pare-feu** : met en place les règles de filtrage

# Chapitre 1 : Topologie et classification des réseaux

Les réseaux sont classifiés selon leur taille en termes de zone de couverture en LAN, MAN et WAN

* **LAN** ou réseau local ou Local Area Network : limité à une entreprise, une administration ou à un utilisateur privé
* **MAN** ou réseau métropolitain pour Metropolitain Area Network : peut s’étendre à l’échelle d’un campus ou d’une ville.
* **WAN** ou Wide Area Network : peut s’étendre à l’échelle d’un pays ou monde
* **Caractéristiques d’un support de transmission :** 
  + **Débit maximal :** nombre de bits/seconde pouvant être transporté sur le support
  + **Type de signal véhiculé :** électrique, lumineux ou ondes électromagnétiques
  + **Atténuation :** affaiblissement du signal le long de la ligne en dB/m
  + **Sensibilité :** aux perturbations électromagnétiques
  + **Couts :** fabrication et installation
* Fibre optique : support de transmission utilisé pour des liaisons longues distances. Cette fibre est **insensible aux perturbations électromagnétiques**
  + **Débit maximal :** vitesse de transmission très élevé
  + **Type de signal véhiculé :** ondes lumineuses
  + **Atténuation :** 0.15 dB/km
  + **Pose délicate : matériau rigide & angle de courbure important**
  + **Couts :** élevé
  + **Poids au mètre faible**
* **Réseaux sans fils** : classifiés selon la taille de zone en couverture
  + **WPAN** ou Wireless Personnal Area Network: **Bluetooth** (faible portée / fort debit)
  + **WLAN** ou Wireless Local Area Network: wifi, Zigbee: Faible débit / Low Power
  + **WMAN** ou Wireless Metropolitain Area Network : destiné principalement aux opérateurs de télécommunication
  + **WWAN ou** Wireless Wide Area Network: reseau cellulaire mobile
    - GSM (Global System for Mobile Communication).
    - GPRS (General Packet Radio Service).
    - EDGE, 3G, 4G
* **Topologies:**
  + **Topologie physique :** désigne la façon dont les ordinateurs sont interconnectés entres eux
  + **Topologie logique :** désigne l’interconnexion interne
* **Caractéristique d’une transmission :** 
  + **Full duplex :** échange bidirectionnel en même temps. Ex : Communication téléphonique, deux ou plusieurs ordinateurs connectés à un périphérique réseau, tel qu’un commutateur (Switch) fournissant l’option full duplex.
  + **Half duplex :** Les données peuvent voyager dans les deux sens mais pas en même temps. Chaque extrémité de la liaison de communication joue le rôle de l’expéditeur et le destinataire (échange bidirectionnel mais **alternativement ;** les données ne peuvent fonctionner que dans une seule direction à la fois ; l’envoi et la réception des données ne se fait pas en même temps.) Ex : TALKIE WALKIE, Hub, …
    - **CSMA/CD : Carrier Sense Multiple Access/Collision Detection** oucircuit de détection de collision
  + **Simplex :** échangeunidirectionnel. Ex : données envoyées à un tableau d’affichage électronique tel que celles trouvées dans les gares et les aéroports
* **Commutation :** c’est le transfert de donnée d’un nœud émetteur à un nœud récepteur
  + **Commutation de circuit :** méthode de transfert de données consistant à établir un **circuit dédié au sein d’un réseau**
  + **Commutation de paquets :** données découpées en paquets de données (segmentation) et **émis indépendamment sur le réseau**
* **Caractéristiques des signaux**
  + **Transmission en bande de base :** les caractéristiques du signal lui permettent d’être transporté en tant que tel sur le support, auquel casle signal est codé et véhiculé sur le support.

**Inconvénients** :

* + - Monopolisation du support
    - Dispersion du spectre (étalement du signal)
    - Sensibilité aux perturbations
* **Transmission en bande transposé ou par modulation :** le canal de transmission utilisé en bande de base étant trop sensible aux perturbations sur de longues distances, on modifie les caractéristiques du signal pour que ce dernier (le signal modifié) puisse être véhiculer sur le support quitte à ce que à la réception qu’on puisse trouver une technique de restitution du signal original. On utilise pour cela des équipements appelés modem (pour modulateur et démodulateur)
* Un modem est un modulateur. La modulation change les caractéristiques du signal au départ et les restitue à l’arrivée (démodulateur)

# Chapitre 2 : Le modèle OSI de l’ISO

* **Protocole**(ensemble de règles) **:** c’est la façon dont sera organisée l’information pour qu’elle soit compréhensible par deux entités distantes.
* **OSI : (Open Systems Interconnection) ou interconnexion de systèmes ouverts**
* **ISO :** International Organization for Standardization
* **Le serveur DNS** (Domain Name System, ou Système de noms de domaine) est un service dont la principale fonction est de traduire un nom de domaine en adresse IP : il convertit les lettres en chiffres.

Les 7 couches du modèle OSI :

* **La couche application** sert d'interface entre les applications et le réseau.
* **La couche présentation** met en forme ou présente les données provenant du périphérique source dans un format compatible pour la réception par le périphérique de destination. Elle permet aussi de compresser les données de sorte que celles-ci puissent être décompressées par le périphérique de destination.
* **La Couche session** crée et gère les dialogues entre les applications source et de destination. Elle redémarre ègalement les sessions interrompues ou inactives pendant une longue période.
* **La couche transport** prépare les données à transmettre sur le réseau. Elle assure la division des données en segments, s'assure qu'aucun des segments n'est perdu et vérifie si tous les segments sont arrivés. Son unité d’information est le **segment**.
* **La couche réseau** fournit des services permettant aux périphériques finaux (ordinateurs, serveurs, etc.) d'échanger des données sur le réseau. Pour effectuer ce transport de bout en bout, la couche réseau utilise quatre processus de base : Adressage des périphériques finaux, Encapsulation, Routage et Désencapsulation. L’unité d’information de la couche réseau est **le paquet IP ou datagramme IP**.
* **La couche liaison de données** accepte les paquets de couche 3, les encapsule dans des unités de données appelées trames, contrôle l'accès au support et détecte les erreurs.
* **La couche physique** fournit un moyen de transporter sur le support réseau les bits constituant une trame de couche liaison de données.

Le standard TCP/IP (Protocole de contrôle de transmission/ Protocole Internet) : il est structuré en 4 niveaux

* **L’interface réseau physique** (couches 1 et 2 du modèle OSI) : dispositifs d’interconnexion et protocole Ethernet.
* **La couche INTERNET** (couche 3 du modèle OSI) : achemine les paquets (routage) d’un ordinateur à un autre.
* **La couche transport** (couche 4 du modèle OSI) : Assure le transport et éventuellement le bon acheminement des paquets.
* **La couche application** (couches 5, 6 et 7 du modèle OSI) : Protocoles d'applications.

# Chapitre 3 : Les éléments d’interconnexion

* **Normalisation** : ensembles des règles
* **Carte réseau** : permet de convertir les signaux venant de support de transmission et allant vers un ordinateur ou les signaux sortant de l’ordinateur et allant vers le support de transmission.

Exemple de cartes réseaux :

* + Carte Ethernet pour les réseaux câblés
  + Carte wifi pour l’accès aux réseaux sans fil
* **Codage en ligne** : processus de conversion de bits en courant électrique dans les réseaux à câble ou en ondes radio dans des réseaux sans fil tel que le wifi.
* **Répéteur** : permet de régénérer le signal d’un même réseau. Il fonctionne au niveau de la couche 1 du modèle OSI.
* **Un HUB** : répéteur à plusieurs ports permettant de connecter plusieurs machines entre elles.

**Fonctions d’un HUB :**

* + Répéter de bloc d’informations d’un segment à l’autre.
  + Régénérer le signal pour compenser l’affaiblissement.
  + Concentrer plusieurs lignes en une seule.

*L’inconvénient est de partager le débit du réseau concerné*

Le répéteur et hub sont des équipements de la couche physique du modèle OSI.

* **Pont**:

Fonctions :

* **Reconnaître** les adresses physiques des informations qui transitent.
* **Filtrer** et laisser passer seulement l’information destiné au réseau raccordé.
* **Assurer** l’interconnexion de stations ou de segments d'un LAN en leur attribuant **l'intégralité** de la bande passante. Le débit disponible **n’est plus partagé** entre tous les utilisateurs.

Il analyse l’entête de niveau 2 (adresse physique)

* **Switch :** c’est un pont à plusieurs ports et fonctionne au niveau de la couche liaison de données du modèle OSI
* **Ponts et Switch** manipulent les **trames** contrairement au répéteur et aux hubs qui manipulent des **bits**
* **Routeur** : permet de relier de nombreux réseaux locaux de sorte à permettre la circulation des datagramme IP d'un réseau à un autre.

Fonctions d’un routeur :

* + **Analyser** et de choisir un chemin à travers le réseau pour véhiculer les paquets sur le réseau
  + **Fragmenter** si nécessaire un datagramme IP pour respecter la taille maximale des données supportée par le réseau sur lequel le datagramme est transféré.

**Le routeur fonctionne au niveau 3 du modèle OSI et par conséquent manipule les datagramme IP.**

* **Normes réseaux locaux :** ETHERNET & RESEAU SANS FIL (Wifi)
  + - **Norme 802.11=norme wifi**
    - **Norme 802.3=norme Ethernet**

Etudier une norme réseau : c’est

* Etudier les équipements qu’on utilise pour mettre en place le réseau en respectant cette norme
* Etudier les supports de transmission
* Etudier les formats de données (de quoi sont constituées ces données)
* Etudier les méthodes d’accès au support. De nos jours, les Switches sont étudiés comme concentrateurs (point de rencontre des différents fils).
* **Normes Ethernet 1** (Ethernet Partagé) : l’équipement d’interconnexion utilise des HUB (écoute de l’équipement, les cartes réseaux font du Half duplex
* **Normes Ethernet 2** (Ethernet commuté) : l’équipement d’interconnexion utilise des SWITCHS

**NB** : la différence entre **Ethernet 1** et **Ethernet 2** est la dernière couche de l’entête.

* Expliquer l’algorithme de réception d’une trame par une carte réseau : une carte réseau écoute
  + C’est quoi écouter et détecter dans notre cas ?
* Quel est l’algorithme de la réception d’une trame par une carte réseau ? (A voir)
* La longueur minimale d’une trame est de 72 octets.

# Chapitre 4 : Couche 2, le protocole Ethernet

Deux principales normes :

* **La norme dite 802.3 ou Ethernet** déployé dans les réseaux câbles
* **La norme 802.11** dont le nom commercial est le **WIFI** pour Wireless Fidelity

Buts de l'étude d'une norme de réseau : c’est

* D’étudier les équipements à utiliser pour déployer un réseau respectant cette norme
* D'étudier les supports de transmission utilisés par un réseau respectant cette norme
* D'étudier aussi les formats de données manipulées dans cette norme.
* D'étudier les méthodes d'accès ou les règles d'accès aux supports de transmission

Les deux sous couches de la couche **Liaison** du modèle OSI :

* **La sous-couche LLC** (norme 802.2) : chargée d’effectuer directement des contrôles sans le concours des couches supérieures
* **La sous-couche MAC** (norme 802.3) : définissant la méthode d’accès au support

**Ethernet partagé** : caractéristiques de la première version (obsolète de nos jours)

* Tous les ordinateurs d'un réseau Ethernet sont reliés à une même ligne de transmission
* Toute machine est autorisée à émettre sur la ligne à n'importe quel moment et sans notion de priorité entre les machines
* Les différents nœuds réseau sont reliés entre eux par un concentrateur (hub) ;
* Un hub transmet sur tous les autres ports ce qu’il reçoit sur un port ;
* A l’extérieur, rien ne le distingue d’un switch

**Ethernet partagé et topologie :**

* **Topologie physique en étoile** : PC connectés à un point central ;
* **Topologie logique en bus** : les données circulent comme si tous les PC étaient connectés sur la même ligne ;

**Principe du CSMA/CD**

* Dans Ethernet partagé, le bus est partagé par toutes les stations.
* Ainsi deux stations émettant en même temps peuvent voir leurs signaux se brouiller : on dit alors qu’il y a **collision**.

Deux stations connectées à un même Hub sont dites **être dans le même domaine de collision**.

Pour résoudre le problème, l’approche CSMA consiste à écouter tout d’abord la porteuse du signal pour savoir si les données y circulent sinon transmettre mais mettre en place un mécanisme pour détecter la collision.

Notons que :

* **CS = Carrier Send** = écoute de la porteuse (le signal)

Avant de transmettre, on écoute le bus pour savoir si des données arrivent.

* **MA = Multiple Access**

Liaison partagée par toutes les machines : **le bus**

* **CD = Collision Detection**

On ne cherche pas à éviter les collisions, on les détecte puis les corrige.

Détection détectée en cas d’émission et de réception simultanées

La version d’Ethernet sans fil (wifi) utilise la méthode CSMA/CA qui consiste à écouter le support avant d’émettre tout en mettant un mécanisme pour éviter les collisions puisqu’il est difficile de les détecter en sans-fil.

Dans la méthode CSMA/CA, **CA signifie Collision** **Avoidance** (évitement des collisions).

* Lors d’une émission de données si une collision est détectée alors on envoie une séquence de 4 octets incohérents pour permettre à toutes les machines du réseau de s’assurer de la collision.
  + Cet envoi de 4 octets incohérents est appelé **brouillage**.
* En cas de détection de collision, pour éviter que plusieurs machines essayent de retransmettre au même moment, elles attendent un temps tiré aléatoirement appelé délai de **BackOff** ou **délai aléatoire après collision**.

Adresse MAC :

* **Une adresse MAC** est un identifiant unique attribué à chaque périphérique réseau (comme une carte Wifi ou Ethernet) par le fabricant. **MAC** signifie **Media Access Control** et chaque identifiant est unique à chaque périphérique.
* Une adresse MAC est codée sur 48 bits (6 octets) et se compose de six groupes de deux caractères chacun, séparés par deux points. Exemple d'adresse MAC : 3c:07:54:3c:75:f9
* L'adresse MAC de diffusion comporte 48 uns (1), représentés au format hexadécimal FF:FF:FF:FF:FF:FF.

**Méthode de réception :**

La méthode de réception mise en œuvre par une interface **Ethernet** peut être décrit comme suit :

1. Écouter sur le bus et attendre qu’une trame arrive
2. Quand une trame est arrivée, on vérifie :
   1. Qu’elle a une longueur ≥ à 72 octets. Si une trame a une longueur de moins de 72 octets c’est qu’elle a subi une collision
   2. Et qu’elle est correcte (reste de la division des champs de la trame par le polynôme générateur = FCS) (en cas de collision le brouillage garantit que la trame sera incorrecte)
3. Si la trame est correcte on regarde ensuite son champ DA (Destination Adresse) :
   1. Si DA = l’adresse de l’interface Ethernet ou FF:FF:FF:FF:FF:FF alors on délivre le champ de Données à la couche supérieure (au système d’exploitation dans le cas d’un paquet IP)
   2. Sinon, la trame n’est pas destinée à l’interface Ethernet et on l’ignore.

**Ethernet commuté**

Ethernet commuté a été mis en place pour résoudre les problèmes que pose Ethernet I à savoir :

* La bande passante est partagée et plus il y a d’hôtes, plus c’est lent
* Comme il ne peut y avoir qu’une trame à la fois sur le support, on travaille en Half-duplex, ce qui est plus lent que le full-duplex (transmission simultanée dans les deux sens)
* Plus il y a d’hôtes, plus les collisions sont fréquentes et ralentissent encore le système

**LE PRINCIPE d’Ethernet commuté :**

* La topologie physique reste en étoile, organisée autour d’un commutateur (switch). Le commutateur utilise un mécanisme de filtrage et de commutation.
* La topologie logique est une étoile
* Le switch inspecte les adresses de source et de destination des trames, dresse une table appelée table de commutation lui permettant de savoir quelle machine (adresse MAC) est connectée sur quel port du switch. La table de commutation se fait par auto-apprentissage.
* Connaissant le port du destinataire, le commutateur ne transmettra la trame que sur le port adéquat, les autres ports restants dès lors libres pour d’autres transmissions pouvant se produire simultanément.
* Il en résulte que chaque échange peut s’effectuer à débit nominal (plus de partage de la bande passante), sans collisions, avec pour conséquence une augmentation très sensible de la bande du réseau (à vitesse nominale égale)
* Puisque la commutation permet d’éviter les collisions et que les techniques 10/100/1000 base T(X) disposent de circuits séparés pour la transmission et la réception (une paire torsadée par sens de transmission), la plupart des commutateurs modernes permet de désactiver la détection de collision et de passer en mode full-duplex sur les ports.
* De la sorte, les machines peuvent émettre et recevoir en même temps (ce qui contribue à nouveau à la performance du réseau)
* Le protocole CSMA/CD est donc devenu obsolète
* Les commutateurs Ethernet modernes détectent également la vitesse de transmission utilisée par chaque machine (autosensing) et si cette dernière supporte plusieurs vitesses (10 ou 100 ou 1000 mégabits/sec), ils entament avec elle une négociation pour choisir une vitesse ainsi que le mode semi-duplex ou full-duplex de la transmission.
* Cela permet d’avoir un parc de machines ayant des performances différentes (par exemple un parc d’ordinateurs avec diverses configurations matérielles)
* Comme le trafic émis et reçu n’est plus transmis sur tous les ports, il devient beaucoup plus difficile d’espionner (sniffer) ce qui se passe
* Voilà qui contribue à la sécurité générale du réseau, qui est un thème fort sensible aujourd’hui
* L’usage de commutateurs permet de construire des réseaux plus étendus géographiquement.

**Auto-construction d’une table de commutation par un switch :**

La table de commutation contient une liste d’enregistrements (adresse MAC, port)

1. **Le switch reçoit une trame Ethernet**
2. **Il vérifie la validité de celle-ci grâce au FCS contenu en fin de trame, si elle est valide on passe au n°3, sinon il la détruit**.
3. **Le switch analyse l’adresse MAC source de la trame.**
   1. Si elle n’est pas présente dans sa table de commutation, il rajoute une nouvelle entrée en l’associant à l’interface par laquelle elle est entrée et lui attribue une durée de vie (300 secondes par défaut sur un switch Cisco)
   2. Si elle est présente et associée à la même interface, le switch rafraîchit la durée de vie.
   3. Si elle est présente mais associée à une autre interface, le switch crée une nouvelle entrée comme s’il s’agissait d’une nouvelle adresse MAC et ensuite supprime l’ancienne entrée.
4. **Le switch analyse l’adresse MAC destination.**
   1. Si l’adresse MAC existe dans la table d’adresse MAC et associée à une interface dans le même vlan que celle d’entrée, le switch propage la trame uniquement par cette interface.
   2. Si l’adresse MAC n’est pas présente dans la table d’adresse MAC, le switch propage la trame par toutes les interfaces du même vlan sauf celle d’où elle provient.
   3. Si l’adresse MAC est soit l’adresse broadcast soit une adresse multicast, le switch propage la trame par toutes les interfaces du même vlan sauf celle d’où elle provient.

**Ethernet :**

* Ethernet est le type de réseau le plus répandu en informatique.
* Ethernet utilise les 3 catégories de supports de transmission :
  + Câbles à paires torsadées
  + Fibre optique
  + Les ondes radios (Wifi)

# Chapitre 5 : Les protocoles de couche3(IP, ARP, ICMP…)

**Protocole IP :**

* **Protocole IP (Internet Protocol)** : un des protocoles les plus importants d'Internet, Il permet de spécifier la destination par une adresse (IP). Mais n’assure pas la livraison : IP est un protocole **non fiable.**
* Besoin d’une machine pour dialoguer sur un réseau :
* D’une adresse IP
* D’un masque de sous réseau.
* D’une **passerelle** : Machine à qui on doit transmettre le paquet lorsque le destinataire n’est pas dans le réseau local.

**Paquet IP**

* **Paquet IP = datagramme IP.**
* Le paquet IP contient les informations nécessaires à la réalisation d’une interconnexion.
* **Le champ de données de la trame Ethernet correspond au paquet IP.**
* **Un datagramme IP** est encapsulé dans une trame Ethernet avant d’être transmis dans un réseau local
* A la réception d’une trame Ethernet par la couche accès réseau du TCP/IP, les données sont extraites et transmises au bon protocole de la couche Internet selon le champ EtherType : c’est le **démultiplexage**
* Le champ EtherType indique le protocole destinataire des **données**

**Composition d’un datagramme IP**

* Un datagramme IP est composé d’une :
  + **en-tête** de taille comprise entre 20 et 60 octets
  + **données IP** nombre quelconque d’octets (limite a 65 315)

**Type d’acheminement désiré :**

* D(elay) : délai d’acheminement court
* T(hroughput) : débit de transmission élevé
* R(eliability) : grande fiabilité

A completer **Réassemblage ??**

**Systèmes de numération :**

* Un groupe de bits est appelé un **mot**, un mot de **huit bits** est nommé un octet (byte).

**Adressage IP :**

* Une adresse IP, universelle ou publique ou routable, est unique au niveau mondial.
* Elle est codée sur **32 bits soit 4 octets,** la notation la plus courante consiste à indiquer chaque octet en décimal et à les séparer par des points. Exemple : 196.1.95.5

Plus précisément, l’adresse IP d’un ordinateur est composée de deux parties :

* La première partie correspond à **l’adresse du réseau ou Net-ID**.
* La deuxième partie correspond à **l’adresse de la machine ou Hots-ID sur le réseau.**

**Attribution d’une adresse IP publique :**

* C'est **l'ICANN** (**Internet Corporation for Assigned Names and Numbers**), qui est chargée d'attribuer des adresses IP publiques.

**Masque de réseau :**

* Un masque de sous-réseau a la même **forme qu'une adresse IP (32 bits**). Il a pour rôle de distinguer le numéro du réseau, du numéro de l'ordinateur dans ce réseau.
* Dès lors qu'un équipement possède une adresse IP, il est extrêmement important de connaître le masque associé afin de déterminer le réseau dans lequel appartient cette machine.
* Par convention, les bits de gauche d'un masque sont à 1 et les bits de droite sont à 0.
  + Exemple : 11111111 11111111 11111111 00000000 ce qui correspond à 255.255.255.0
* Pour connaître le réseau dans lequel appartient une machine, on fait un & logique entre le masque de sous réseau et l’adresse IP de la machine.
  + Exemple :
* Une machine possède l'adresse IP : 194. 214. 110. 35
* Elle possède un masque : 255. 255. 255. 0
* L'adresse du réseau est : 194. 214. 110. 0
* L'adresse de cette machine dans le réseau est : 35
* Dans chaque réseau, les adresses dont les bits de machine sont tous à 0 (valeur 0) ou tous à 1 (valeur 255) ne peuvent être attribuées :
  + Tous les bits à ‘0’ désigne le réseau dans son ensemble
  + Tous les bits à ‘1’ représente l’adresse de diffusion (broadcast) à destination de tous les nœuds du réseau.
  + Une machine dans un réseau IP utilise son masque de réseau pour savoir si une autre machine dont elle connaît l'adresse IP se trouve dans son réseau ou non. De manière précise, si une machine A dont l'adresse IP est IPA veut initier une communication vers une machine dont l'adresse IP est IPB alors le processus suivant est mis en œuvre par A pour savoir si B se trouve sur ce réseau ou pas :
* A applique son masque de réseau NMA à son adresse IP pour obtenir son adresse réseau notée IPRXA
* A applique aussi son masque de réseau NMA à l'adresse IP de B pour obtenir l'adresse réseau de B notée IPRXB
* SI IPRXA = IPRXB alors A se dit qu'elle se trouve dans le même réseau que B.
* Si IPRXA est différente de IPRXB alors A se dit qu'elle ne se trouve pas dans le même réseau que B ; dans ce cas la communication entre A et B n'est possible que par l'intermédiaire d'une passerelle (par défaut).

# Chapitre 6 : Le routage IP

# Chapitre 7 : Les protocoles de couche 4 (TCP, UDP…)

**Préliminaire :**

* Dans un réseau IP, les applications sont identifiées par le couple (**adresse IP, numéro du port**)
* Socket : un socket peut être vu comme une attente de disponibilité des moyens de transports (file d’attente).
* **Flux réseau :** c’est un ensemble de paquets quittant la même source et allant à la même destination
* Les protocoles de transports TCP et UDP ont été défini pour pallier aux limitations d’IP telles que :
  + **la non garantie de livraison de datagramme IP**
  + **les erreurs non signalées**
  + **dé-séquencement possibles des datagrammes**
  + **la non prise en charge des mécanismes de détection des erreurs sur les données**
  + **la non gestion de contrôle de flux**
  + **et surtout le non adressage des applications clients/serveurs**

Ces protocoles de transport ont été définis pour pouvoir corriger les erreurs signalées par **ICMP** comme celles qui ne sont pas signalées

* Ainsi, de manière précise l’adresse d’une application dans un réseau IP est le triplet (**Adresse IP, Protocole de transport et numéro du port**).
* Quand la couche réseau reçoit un datagramme IP sur une machine destinataire, elle examine le champ protocole du datagramme IP pour savoir à quel protocole de transport remettre les données (17 si UDP, 6 si TCP)

**Protocole UDP :**

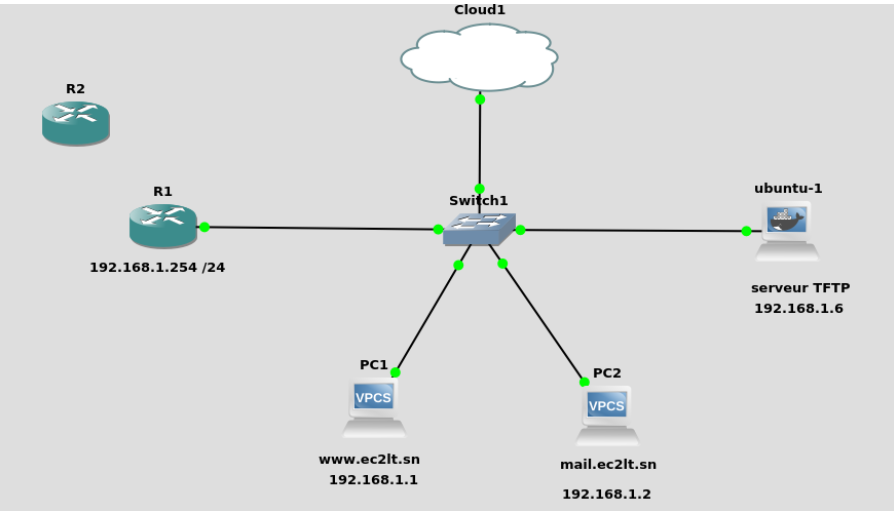
* Le protocole fonctionne en mode **non connecté** (possibilité de pertes, dé-séquencement des messages, duplication, la non régulation des flux) et rend les services suivants :
  + envoi/réception de messages entre applications (processus) à travers Internet
  + adressage des applications par numéro de port
  + multiplexage/démultiplexage par numéros de port
  + contrôle facultatif de l’intégrité des données
* Certains ports UDP sont réservés pour des applications particulières :
  + Les ports [1, 1023] sont réservés et ne sont jamais à utiliser
  + les ports [1024, 49151] sont enregistrés (mais peuvent être utilisés)
  + les ports [49152, 65535] sont dits dynamiques et/ou à usage privé
* Champs UDP : Checksum
  + Ce champ permet de vérifier l’intégrité de la totalité du datagramme IP.
  + Il permet également de s’assurer que :
    - Les données reçues sont correctes
    - les ports sont corrects
    - les adresses IP sont correctes
* Un **serveur** est un dispositif informatique (matériel et logiciel) qui offre des services à un ou plusieurs clients (parfois même des milliers).
* Un **service** est un couple client-serveur
* Le protocole ou environnement ***client–serveur*** désigne un mode de transaction (souvent à travers un réseau) entre plusieurs programmes ou processus : l'un, qualifié de *client*, **envoie des requêtes** ; l'autre, qualifié de *serveur*, **attend les requêtes des clients et y répond.**
  + **Navigateur :** client d’un serveur
* Le serveur est démarré sur un ordinateur en écoute sur un port. Son adresse est le triplet : (adresse IP, UDP, port)

Quelques services de base :

* **ftp**(file transport Protocol) : permet de transférer des fichiers. Il utilise 2 ports :
  + **20 pour les requêtes**
  + **21 pour les données**
* **Secure shell ssh**: assure une authentification forte et des communications de données chiffrées sécurisées entre deux ordinateurs connectés sur un réseau peu sûr, tel qu'Internet. Il utilise le port 22 et le protocole TCP
* **telnet**: protocole de connexion à distance non sécurisé. Il utilise protocole de transport TCP et le port 23
* **smtp** (simple mail transport protocol) : protocole de transport de mail. Port : 25
* **domain** (domain name server) : utilise les protocoles TCP Et UDP, et le port 53
* **tftp** (Trivial File Transfert Protocol ) : est un protocole simplifié de transfert de fichiers. Il fonctionne en UDP sur le port 69.

Il permet de sauvegarder des fichiers de configuration de Routeurs, etc.

Par exemple, on peut installer n machines avec ce serveur tftp en même temps.



* **kerberos :** est un service d'authentification qui est utilisé sur les réseaux informatiques ouverts ou non sécurisés. Il utilise les protocoles TCP & UDP, et le port 88
* **pop3** (post office protocol) : sert à télécharger des mails ; protocole TCP & port 110
* **imap2** (internet mail access protocol) : permet d’accéder à ses mails sans pour autant les télécharger ; port 143
* **https :** les données sont cryptées avant d’être envoyer
* **DHCP**: protocole UDP ; port 67

Un serveur DHCP (ou service DHCP) est un serveur (ou service) qui délivre des adresses IP aux équipements qui se connectent sur le réseau.

DHCP est l’abréviation de Dynamic Host Configuration Protocol (en français : Protocole de Configuration Dynamique d’Hôte

* **DNS**: protocoles : TCP/UDP ; port 53

**Le protocole TCP (Transport Control Protocol) :**

* Le protocole de transport **TCP** fonctionne en **mode connecté.**
* Le protocole de transport TCP est un protocole fiable avec des propriétés suivantes :
  + **Orienté connexion** : transfert de flots d’octets. La suite d’octets remise au destinataire est la même que celle émise.
  + **Circuits virtuels** : une fois une connexion demandée et acceptée, les applications la voient comme un circuit dédié
  + **Transferts tamponnés** : quelle que soit la taille des blocs de données émis par les applications, TCP est libre de les découper ou de les regrouper
  + **Connexions non structurées** : pas de frontière placée par TCP entre les messages émis par les applications
  + **Connexions full-duplex** : les données s’échangent dans les deux sens (mais un côté peut libérer un sens de transmission quand il n’a plus de données à émettre)

**Adresse d’application, port et connexion**

* Comme pour UDP, l’adresse d’une application est un triplet (**adresse IP, TCP, port**) : le serveur et le client doivent en posséder une. Le port du client est généralement quelconque.
* Mais à la différence d’UDP, on ne peut envoyer un message directement à une adresse : il faut que le client établisse une connexion avec le serveur. Ils ne peuvent échanger des messages que via une connexion
* **Établissement d’une connexion** :
  + Serveur : effectue une ouverture passive en écoutant sur un port, c’est à dire en demandant un port et en attendant qu’un client s’y connecte.
  + Client : effectue une ouverture active en demandant l’établissement d’une connexion entre son adresse et celle du serveur. Le serveur doit être en écoute. Les modules TCP du client et du serveur interagissent pour établir cette **connexion.**
* Une fois la connexion établie, le serveur et le client doivent l’utiliser pour envoyer/recevoir des messages. TCP est chargé d’assurer la fiabilité de la connexion (notamment s’occupe des acquittements/ retransmissions)

**Ports réservés TCP :**

* Certaines applications bien connues ont des ports TCP réservés [0, 1023].
* Une connexion est identifiée par le quadruplet formé avec l’adresse de ses deux extrémités : (adresse IP locale, port local, adresse IP distante, port distant)

**Segment TCP : Checksum**

* Ce champ est obligatoire et permet de vérifier la totalité de l’intégrité du segment + son Pseudo en-tête TCP. Comme pour UDP, ce champ permet de s’assurer :
  + que les données sont correctes
  + que les ports sont corrects
  + que les adresses IP sont correctes

**Segment TCP : option MSS**

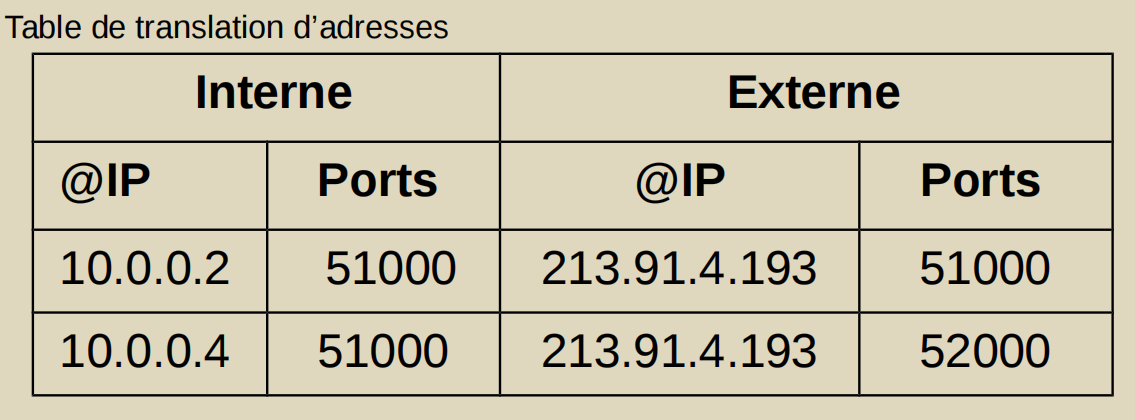
* Le champ option MSS n’est utilisé que pendant la phase de connexion et sa taille est de 4 octets
* Chaque côté de connexion indique la taille maximale des données des segments appelé MSS (Maximum Segment Size) qu’il veut recevoir :
* généralement MSS est fixé à MTU - 40 (en-têtes IP et TCP sans option)
* MSS dépend aussi de la taille des buffers de réception
* par défaut sa taille est de 536 octets
* MSS est difficile à choisir sur l’Internet :
* si elle est trop petite alors on peut avoir une perte d’efficacité
* si elle est trop grande alors il y a risque de fragmentation des datagramme IP contenant des segments

**Translation d’adresses :**

* Le mécanisme de translation d'adresses (Network Address Translation noté NAT) a été mis au point afin de répondre à la pénurie d'adresses IP avec le protocole IPv4.
* Cela consiste donc à utiliser une passerelle de connexion à internet, possédant au moins une interface réseau connectée sur le réseau privé et au moins une interface réseau connectée à Internet (possédant une adresse IP routable).
* C’est le cas des **routeurs ADSL** utilisés au Sénégal qui ont une adresse IP publique et une interface connectée au réseau privé des abonnés de la SONATEL (Société Nationale des Télécommunications).
  + Lorsqu’ une machine dans le réseau privé veut envoyer des paquets sur internet, l’adresse IP source du paquet sortant sur l’interface publique du routeur qui fait le NAT est remplacée par l’adresse IP publique du routeur.
  + En revanche, les paquets reçus d’internet par le routeur résultant des requêtes émises du réseau privé voient leur adresse de destination remplacée par une adresse du réseau privé avant que ceux-ci ne soient retransmis à leur destinataire dans le réseau privé.
* Une connexion vers une application nécessite le quadruplet (adresse IP source, port source et adresse IP destination, port destination)

**Les paquets rentrants**

Pour retrouver les adresses IP des paquets IP qui reviennent au client,

* Le routeur NAT utilise une table de correspondance appelé table de NAT qui est construite de manière dynamique comme le montre le tableau suivant :
* Par exemple si le routeur NAT reçoit des demandes de connexion des machines 10.0.0.2 et 10.0.0.4 avec des ports sources confondus 51000 alors pour éviter des confusions le routeur décide d’associer le port 52000 comme port source de requête de la machine 10.0.0.4.
* Ainsi si un paquet venant d’internet allant vers le port 51000 du routeur NAT sera redirigé vers la machine 10.0.0.2 port 51000 alors un paquet venant d’internet et allant vers le port 52000 du routeur NAT sera redirigé sur le port 51000 de la machine 10.0.0.4.
* Ce mécanisme de translation de port est appelé **PAT** (Port Address Translation) utilisé par des routeurs ADSL ne possédant qu’une seule adresse IP publique à un instant donné.

**Trois types de translation d’adresses** :

* **NAT statique** : à une adresse IP source dans le privé on associe une adresse et une seule adresse IP publique.
* **NAT dynamique** : on définit une plage d’adresses IP publique qu’on attribue à des machines qui initient des connexions vers l’extérieur
* **PAT** : une seule adresse IP publique est utilisée pour toutes les connexions sortantes quel que soit la machine dans le réseau privé mais à chaque requête on associe un numéro de port.