Réseaux

1 Notion de réseau informatique

1.1 Histoire

Les réseaux existaient avant l'informatique. Un exemple notable est la transmission optique avec des bras articulés du Français Claude Chappe au XVIII^{e} siècle.
Voici deux vidéos pour l'histoire des réseaux en général :

— Une vidéo courte donnant un bon aperçu

— Une excellente vidéo du National Géographic qui insiste sur la transmission optique

Ce qui nous intéresse ce sont les réseaux informatiques.
On sait transmettre de l'information avec de l'électricité depuis 1844, et sans fil avec des ondes électromagnétique (ondes radios) depuis 1896 avec la naissance de la télégraphie sans fil (TSF).
L'information est codé par la présence ou non d'un signal (un voltage sur le fil). Avec les ordinateurs qui apparaissent dans les années 1950, le problème est de faire communiquer plusieurs ordinateurs en les reliant sur un même réseau, ce qui suppose plusieurs choses :

— L'établissement de protocole pour que tous les ordinateurs parlent le même langage sur le réseau.

— La mise au point d'un système d'adresses et de routage pour orienter les messages vers leur destinataires final.

Pour les protocoles, le principe de la transmission de paquets est introduit par Paul Baran et Davies en 1961 : il consiste à découper les données en paquets, ce qui permet de transmettre avec un débit variable (un courriel nécessite l'envoi ponctuel de petits paquets alors que pour transférer un fichier, il faut envoyer rapidement de gros paquets).

Arpanet, le projet de réseau interuniversitaire financé par l'Arpa (agence de recherche de la défense américaine) , voit le jour en 1969 sous la direction de Leonard Kleinrock : les données sont découpées en paquets, transmis en séquence les uns à la suite des autres.

Le routage apparaît dans les années 70 : Louis Pouzin, après un séjour au MIT, développe en France le réseau Cyclades qui est le premier véritable réseau à commutation de paquets : les paquets transitent de

façon indépendante dans le réseau grâce à un protocole qui préfigure Internet Protocol puis sont remis en l'ordre à l'arrivée. Le circuit des paquets est donc variable contrairement à la commutation de circuits implémentée dans le réseau téléphonique.

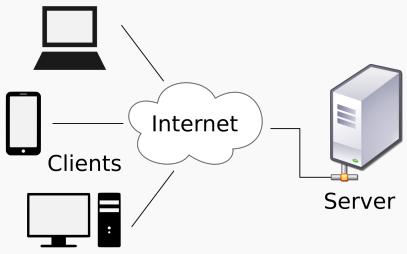
Aux États-Unis, Vinton Cerf et Robert Kahn s'inspirent des idées de Pouzin et inventent les protocoles IP et TCP. C'est ce protocole (en version 4 (1982) et 6 (1995)) qui est encore utilisé de nos jours pour coder l'information et acheminer les messages à leur destination. L'interconnexion des réseaux Arpanet et Csnet en 1983 avec TCP/IP marque la naissance d'Internet et son expansion au niveau mondial dans les sphères universitaires et de la recherche.

En 1989, Tim Berners-Lee invente le Web qui est une application de documents hypertextes s'exécutant par-dessus le réseau Internet. L'ouverture des protocoles Web au grand public en 1993 connaît un succès fulgurant, d'autres services Internet comme le mail ou le transfert de fichier de pair à pair se popularisent aussi. Le trafic Internet explose : de quelques mégabits par seconde en 1992, on est passé à près de 100 térabits par seconde en 2018 avec près de 3,2 milliards d'internautes en 2016.

1.2 Terminologie et classification des réseaux

Définition 1 : terminologie

1. Un réseau est un ensemble de noeuds reliés par des liens et correspond mathématiquement à un graphe. Dans un réseau informatique les noeuds ou hôtes sont des équipements informatiques comme des ordinateurs, des routeurs... et les liens peuvent être variés selon la technologie utilisée : filaire (Ethernet,...) ou par ondes (Wifi,...).
2. Une interface est le point de raccordement, matériel (carte réseau) ou logiciel, entre un lien et un noeud.
3. Un protocole est un ensemble de règles permettant d'établir une communication entre deux noeuds du réseau et de garantir éventuellement certains services (fiabilité, confidentialité...)
4. Un service réseau est une application capable de communiquer en réseau et proposant des fonctionnalités. Par exemple, un service Web peut fournir des pages Web au navigateur d'un client. Sur un réseau pédagogique de lycée, un service de gestion et de partage de fichiers permet aux utilisateurs d'accéder à leurs fichiers depuis n'importe quel machine cliente.
5. Un serveur désigne un matériel ou un logiciel exécutant un service réseau. Il fournit un service à des clients selon une architecture client/serveur. Pour une présentation de l'architecture client-serveur, on pourra visionner cette vidéo.

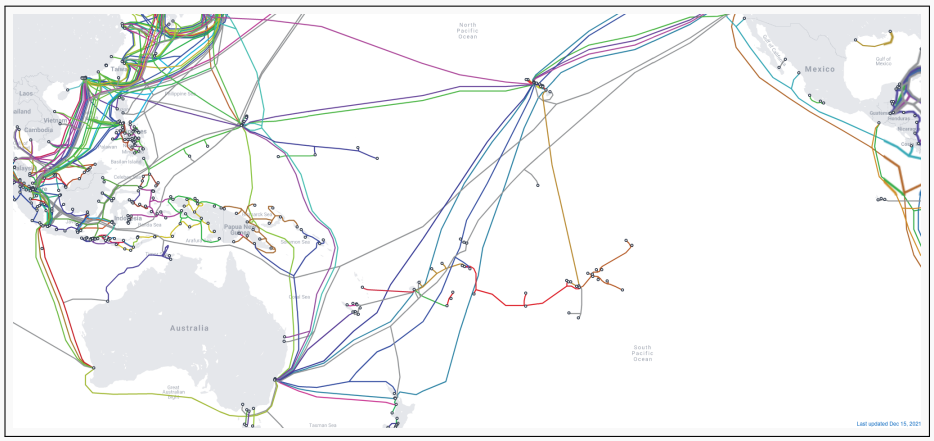


Définition 2 : classification des réseaux

1. Les réseaux informatiques peuvent être de différentes tailles :
   - les réseaux locaux ou Local Area Network (LAN) limités à une zone géographique restreinte (maison, entreprise, lycée...)
   - les réseaux étendus ou Wide Area Network (WAN) couvrant de vastes zones géographiques (pays, continent). Ce sont, par exemple, les réseaux des fournisseurs d'accès internet (Free, Orange, SFR...), de grandes sociétés...

   Internet est une interconnexion mondiale de réseaux.
2. Les réseaux informatiques utilisent des liens de technologies diverses :
   - des liaisons filaires : câbles en cuivre à paires torsadées, fibres optiques ...
   - des liaisons par ondes : Wifi, Bluetooth, satellite, parabole entre deux antennes (Rangiroa et Tikehau), 4G...

3. L'interconnexion dans l'Internet de tous ces réseaux hétérogènes sur le plan matériel a été rendu possible par le développement de protocoles logiciels. Pour une présentation globale d'Internet, on pourra visionner cette vidéo.



Carte des câbles sous-marins – https://www.submarinecablemap.com/

Exercice 1 : QCM type E3C

1. Un protocole est un ensemble de...
   (a) matériels connectés entre eux
   (b) serveurs et de clients connectés entre eux
   (c) règles qui régissent les échanges entre équipements informatiques
   (d) règles qui régissent les échanges entre un système d'exploitation et les applications
2. Comment s'appelle l'ensemble des règles qui régissent les échanges sur Internet ?
   (a) les couches
   (b) le wifi
   (c) les protocoles
   (d) les commutateurs
3. L'architecture client-serveur :
   (a) est un mode de communication entre programmes
   (b) est une architecture matérielle de coopération entre machines
   (c) est un mode de communication entre routeurs
   (d) est un mode de communication entre commutateurs

2 Architecture d'un réseau

2.1 Adresse MAC et IP

Sur le réseau physique, c'est à dire le même switch ethernet, ou la même antenne wifi, les machines s'échangent des paquets en utilisant les adresses MAC. Sur un réseau plus grand, dès que l'on doit passer par un routeur, et en particulier sur l'internet mondial, on utilise une adresse IP.

Définition 3 : adresse MAC

Chaque interface sur le réseau dispose d'une adresse MAC qui est une valeur unique attribuée à la carte réseau (Ethernet, Wifi, 4G, 5G, ...) lors de sa fabrication en usine, ou changée plus tard (vois plus bas).

Cette adresse est codée sur 48 bits (présentés sous la forme de 6 octets en hexadécimal), par exemple `fc:aa:14:75:45:a5`. Les trois premiers octets correspondent au code du fabricant. Un site comme https://www.macvendorlookup.com/ permet de retrouver le fabricant d'une adresse MAC quelconque.
Les adresses MAC sont souvent utilisés pour autoriser des machines spécifiques (laptop ou téléphone) à utiliser un réseau... mais on peut changer les adresses MAC avec la plupart des cartes réseaux modernes et les téléphones et tablettes utilisent aujourd'hui par défaut des adresses MAC aléatoires qui changent périodiquement. Tout ceci pause souvent des problèmes de connexions.

Définition 4 : adresse IP

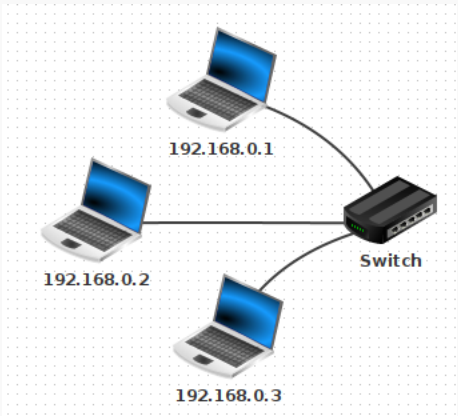
Une adresse IP est aussi une valeur unique attribuée à chaque interface. Elle est sur 32 bits en IPV4 (version 4 de IP) et sur 128 bits en IPV6.
On écrit en général les adresses IPV4 en groupant les 32 bits en 4 octets que l'on donne en décimal. Ex : 192.168.0.1. Une adresse IPV6 s'écrit avec 8 paquets de 16 bits en héxadécimal, avec omission des zéros consécutifs au milieu. Ex : fe80 ::42 :2dff :fe26 :1c7f signifie fe80 :0000 :0000 :0000 :0042 :2dff :fe26 :1c7f.
La relation entre le nom d'une machine (ex : google.com) et sa (ou ses) adresses IP (142.250.68.46 ou 2607 :f8b0 :4007 :810 ::200e pour google.com, le jour où ce document a été écrit) est la charge des serveurs de noms (DNS : domain name server), et le passage de l'adresse IP à l'adresse MAC est géré par le protocole ARP (Address Resolution Protocol). ARP ne nécessite en général pas de configuration.

Le réseau internet mondial connait depuis les années 2000 une pénurie d'adresse IPV4 (il n'y en a que 4 milliards environ) et le passage global à IPV6 qui est un standard accepté par les autorités depuis 1998 se fait attendre ... Cette pénurie rend impossible d'assigner une adresse visible mondialement à toutes les machines du monde. On utilise alors des redirections de ports et autres techniques pour accéder aux machines d'un réseau local qui n'ont pas d'IP connue à l'extérieur. Cela complexifie la tâche des administrateurs et diminue les performance du réseau.
IPV6 simplifie énormément les choses car les 48bits de droites de l'IPV6 sont l'addresse MAC, les 64 bits de droites (donc l'addresse MAC + 16 bits) sont l'adresse sur le réseau local et les 64 bits de gauche l'adresse du réseau local lui même. On dispose ainsi potentiellement de 16 milliars de milliard d'adresses pour les réseaux locaux et autant pour le nombre de machine sur chaque réseau. IPV6 rendrait par exemple beaucoup plus facile le jeu en réseau !

2.2 Un premier réseau local

Activité 1

1. À l'aide du logiciel Filius, créer le réseau local ci-dessous :

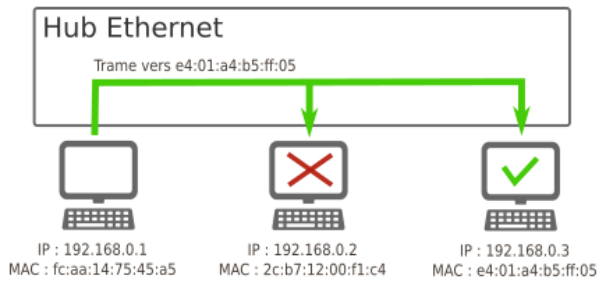


2. Tester alors le de la machine `192.168.0.1` vers la machine `192.168.0.3`.

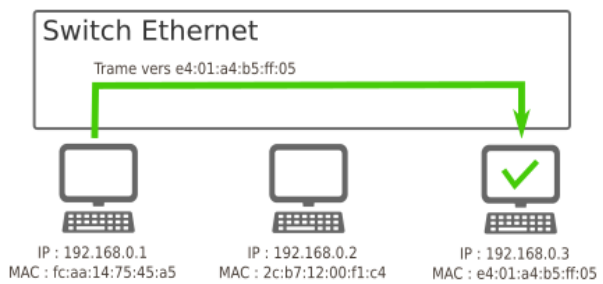
```
root /> ping 192.168.0.3
PING 192.168.0.3 (192.168.0.3)
From 192.168.0.3 (192.168.0.3): icmp_seq=1 ttl=64 time=413ms
From 192.168.0.3 (192.168.0.3): icmp_seq=2 ttl=64 time=204ms
From 192.168.0.3 (192.168.0.3): icmp_seq=3 ttl=64 time=205ms
From 192.168.0.3 (192.168.0.3): icmp_seq=4 ttl=64 time=203ms
--- 192.168.0.3 Statistiques des paquets ---
4 paquets transmis, 4 paquets reçus, 0% paquets perdus
```

Définition 5 : différences entre switch (ou commutateur) et hub

1. Au sein d'un hub Ethernet (de moins en moins vendus), il n'y a aucune analyse des données qui transitent : il s'agit simplement d'un dédoublement des fils de cuivre (tout comme une multiprise électrique). L'intégralité des messages est donc envoyée à l'intégralité des ordinateurs du réseau, même s'ils ne sont pas concernés.



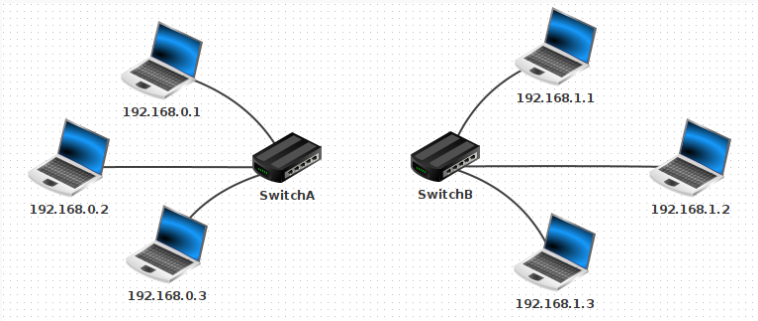
2. Au sein d'un switch Ethernet , une analyse est effectuée sur la trame qui est à distribuer. Lors du branchement d'un nouvel ordinateur sur le switch, celui-ci récupère son adresse MAC, ce qui lui permet de trier les messages et de ne les distribuer qu'au bon destinataire.



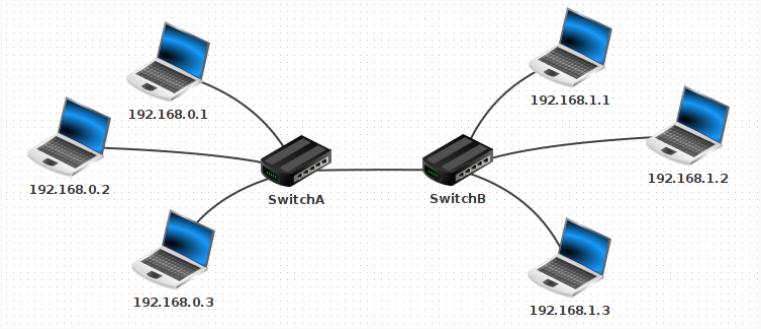
2.3 Un deuxième sous-réseau

Activité 2

1. Ajouter un deuxième sous-réseau (penser à bien renommer les switchs) :



2. Relier ces deux sous-réseaux à l'aide d'un câble :



   (a) Essayer de « pinger » la machine `192.168.1.2` depuis la machine `192.168.0.1`. Que se passe-t-il ?

   (b) Temporairement, changer l'adresse IP de la machine `192.168.1.2` en `192.168.0.33` puis essayer à nouveau le ping depuis la machine `192.168.0.1`.

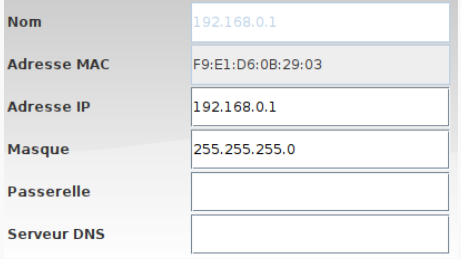
Remarque

Dans le premier cas, le ping n'aboutissait pas car les machines `192.168.1.2` et `192.168.0.1` ne sont pas dans le même sous-réseau. Dans le second cas, le ping aboutit car les machines `192.168.0.1` et `192.168.0.3` sont dans le même sous-réseau.

Comment savoir si deux machines sont dans le même sous-réseau ?

Méthode 1 : explication basique

Dans Filius, lors de l'attribution de l'adresse IP à une machine, une ligne nous permet de spécifier le masque de sous-réseau (appelé simplement « Masque » dans Filius). C'est ce masque qui va permettre de déterminer si une machine appartient à un sous-réseau ou non, en fonction de son adresse IP.



— Avec comme masque `255.255.255.0`, toutes les machines ayant une adresse IP commençant par les trois mêmes premiers nombres appartiendront à un même sous-réseau. Comme ceci

est le réglage par défaut de Filius, cela explique pourquoi `192.168.0.33` et `192.168.0.1` sont sur un même sous-réseau, et pourquoi `192.168.1.2` et `192.168.0.1` ne sont pas sur un même sous-réseau.
Dans cette configuration, 256 machines peuvent donc appartenir au même sous-réseau (ce n'est pas tout à fait le cas car des adresses finissant par 0 ou par 255 sont réservées).

— Avec comme masque `255.255.0.0`, toutes les machines ayant une adresse IP commençant par les deux mêmes premiers nombres appartiendront à un même sous-réseau.
Dans cette configuration, 65 536 machines peuvent être dans le même sous-réseau (car $256^2 = 65\,536$).

Activité 3

1. Renommer `192.168.0.33` en `192.168.1.2` et modifier son masque en `255.255.0.0`.
2. Modifier aussi le masque de `192.168.0.1` en `255.255.0.0`.
3. Avec ces modifications, que peut-on dire du ping de `192.168.0.1` vers `192.168.1.2` ? Vérifier votre réponse.

Méthode 2 : explication « avancée »

Lorsqu'une machine A veut envoyer un message à une machine B, elle doit déterminer si cette machine :

— appartient au même sous-réseau, auquel cas le message est envoyé directement via un ou plusieurs switchs ;

— n'appartient pas au même sous-réseau, auquel cas le message doit d'abord transiter par un routeur.

En notant et les adresses IP respectives des machines A et B, et le masque de sous-réseau :

A et B appartiennent au même sous-réseau si, et seulement si, .

Exercice 2

Compléter le tableau suivant et déterminer quelles machines font partie d'un même sous-réseau :

Machine A	Machine B	Machine C
`192.168.129.10`	`192.168.135.200`	`192.168.145.1`
`255.255.248.0`	`255.255.248.0`	`255.255.248.0`

Définition 6 : notation CIDR

D'après ce qui précède, 2 informations sont nécessaires pour déterminer le sous-réseau auquel appartient une machine : son IP et le masque de sous-réseau. Une convention de notation permet d'écrire simplement ces deux renseignements : la notation CIDR.

Une machine d'IP `192.168.0.33` avec un masque de sous-réseau `255.255.255.0` sera désignée par `192.168.0.33/24` en notation CIDR.
Le suffixe `/24` signifie que le masque de sous-réseau commence par 24 bits consécutifs de valeur 1 : le reste des bits (donc 8 bits) est mis à 0. Autrement dit, ce masque vaut `11111111.11111111.11111111.00000000` , soit `255.255.255.0`.

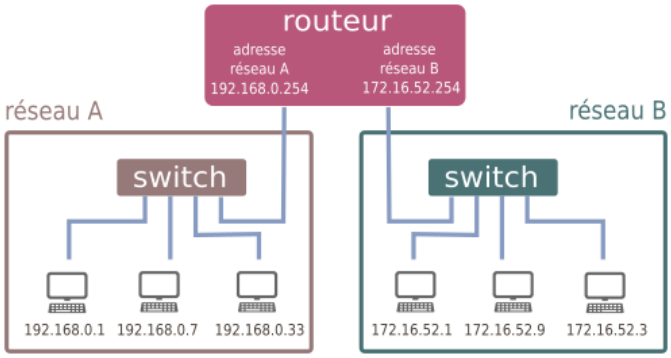
Exercice 3

De la même manière, déterminer les masques correspondant aux suffixes `/16` et `/21`.

2.4 Nécessité d'un routeur

La solution initiale (relier les deux switchs par un cable pour unifier les deux sous-réseaux) n'est pas viable à l'échelle d'un réseau planétaire.

Pour que les machines de deux réseaux différents puissent être connectées, on va utiliser un dispositif équipé de deux cartes réseaux situé à cheval entre les deux sous-réseaux. Cet équipement de réseau est appelé routeur.



Principe de fonctionnement d'un routeur

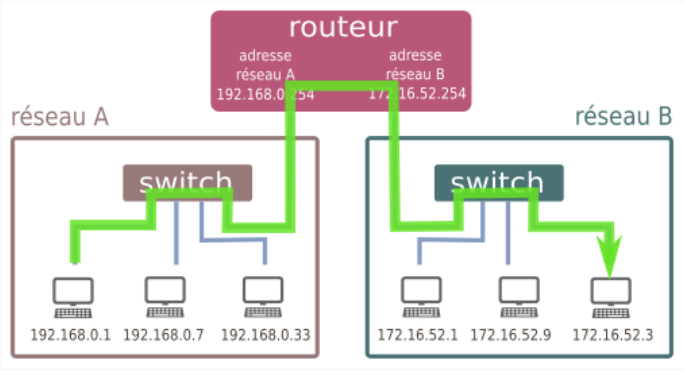
Imaginons que la machine `192.168.0.1/24` veuille communiquer avec la machine `172.16.52.3/24`.

L'observation du masque de sous-réseau de la machine `192.168.0.1/24` nous apprend qu'elle ne peut communiquer qu'avec les adresses de la forme `192.168.0.X/24`, où `X` est un nombre entre 0 et 255.

Voici les 3 étapes du routage :

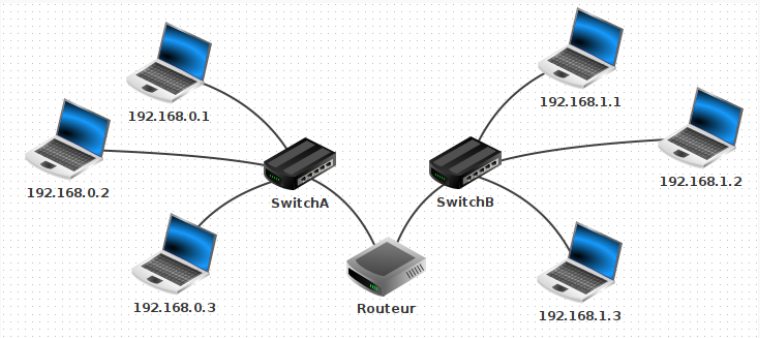
1. Lorsque qu'une machine A veut envoyer un message à une machine B, elle va tout d'abord vérifier si cette machine appartient à son réseau local. Si c'est le cas, le message est envoyé par l'intermédiaire du switch qui relie les deux machines.
2. Si la machine B n'est pas trouvée sur le réseau local de la machine A, le message va être acheminé vers le routeur par l'intermédiaire de son adresse de passerelle (qui est bien une adresse appartenant au sous-réseau de A).
3. De là, le routeur va regarder si la machine B appartient au deuxième sous-réseau auquel il est connecté. Si c'est le cas, le message est distribué, sinon, le routeur va donner le message à un autre routeur auquel il est connecté et va le charger de distribuer ce message : c'est le procédé (complexe) de routage qui sera vu en classe de Terminale.

Dans notre exemple, l'adresse `172.16.52.3` n'est pas dans le sous-réseau de `192.168.0.1`. Le message va donc transiter par le routeur.

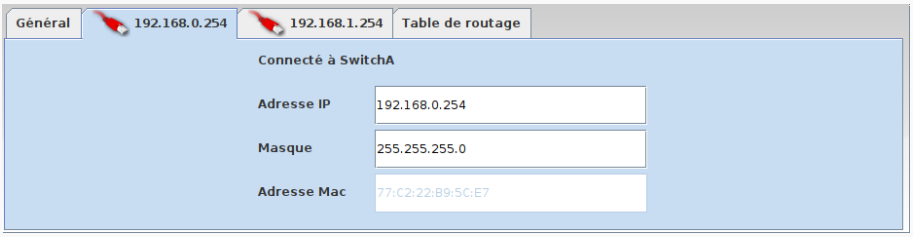


Activité 4 : illustration avec Filius

1. Ajouter un routeur entre le `SwitchA` et le `SwitchB`.



2. Configurer le routeur de la façon suivante :
   (a) adresse `192.168.0.254` pour l'interface reliée au `SwitchA` ;
   (b) adresse `192.168.1.254` pour l'interface reliée au `SwitchB` ;
   (c) dans l'onglet `Général`, sélection « Routage automatique ».



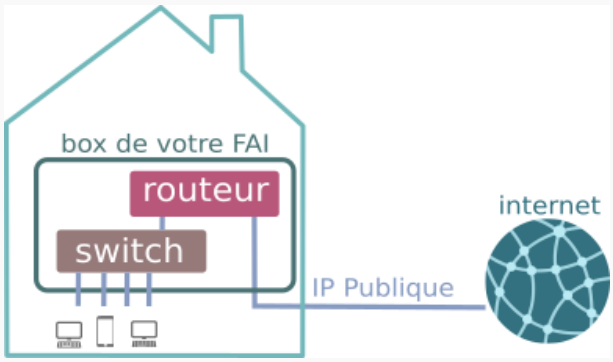
   Ainsi configuré, le routeur peut jouer le rôle de passerelle entre les deux sous-réseaux.
3. Essayer le ping entre `192.168.0.1` et `192.168.1.2`.
4. Configurer correctement la passerelle des deux machines précédentes, et essayer à nouveau.
5. Effectuer un `traceroute` entre les deux machines.

Cas d'un réseau domestique

Dans le cas d'un réseau domestique, la box de l'opérateur joue simultanément le rôle de switch et de routeur :

— switch car elle répartit la connexion entre les différents dispositifs (ordinateurs branchés en ethernet, smartphone en wifi, tv connectée...) ;

— routeur car elle fait le lien entre ce sous-réseau domestique (les appareils de votre maison) et le réseau Internet.



Les commandes ipconfig (Windows) et ip (Linux)

Les commandes `ifconfig` ou `ip address` sous Linux ou `ipconfig` sous Windows permettent d'afficher les adresses physique (MAC) ou logique (IP) d'une interface réseau.

Exercice 4

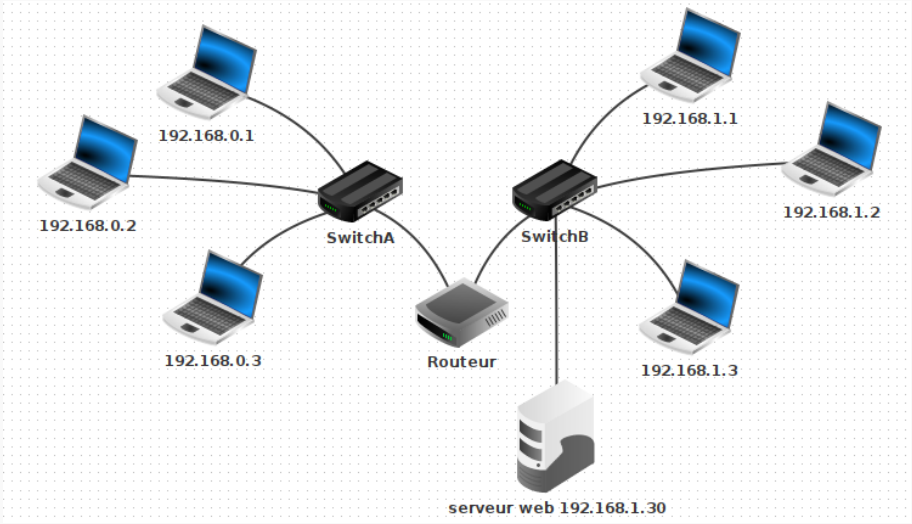
Voici par exemple ce que donne `ip adress` :

```
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: enp2s0f0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc pfifo_fast state DOWN group default qlen 1000
    link/ether 54:05:db:6f:8e:3f brd ff:ff:ff:ff:ff:ff
3: enp4s0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc pfifo_fast state DOWN group default qlen 1000
    link/ether 54:05:db:6f:8e:3e brd ff:ff:ff:ff:ff:ff
4: wlp3s0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen 1000
    link/ether c8:e2:65:32:7e:77 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.86/24 brd 192.168.1.255 scope global dynamic noprefixroute wlp3s0
       valid_lft 72677sec preferred_lft 72677sec
    inet6 fe80::a41f:f1ac:95b2:b4b2/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
5: enp6s0f3u1u1: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc pfifo_fast state DOWN group default qlen 1000
    link/ether 48:2a:e3:82:a7:17 brd ff:ff:ff:ff:ff:ff
```

Lire l'adresse MAC et l'adresse IP de l'interface `wlp3s0`.

Activité 5 : serveur web

1. Connecter un ordinateur au `SwitchB`, sur l'adresse `192.168.1.30` et y installer un serveur web.



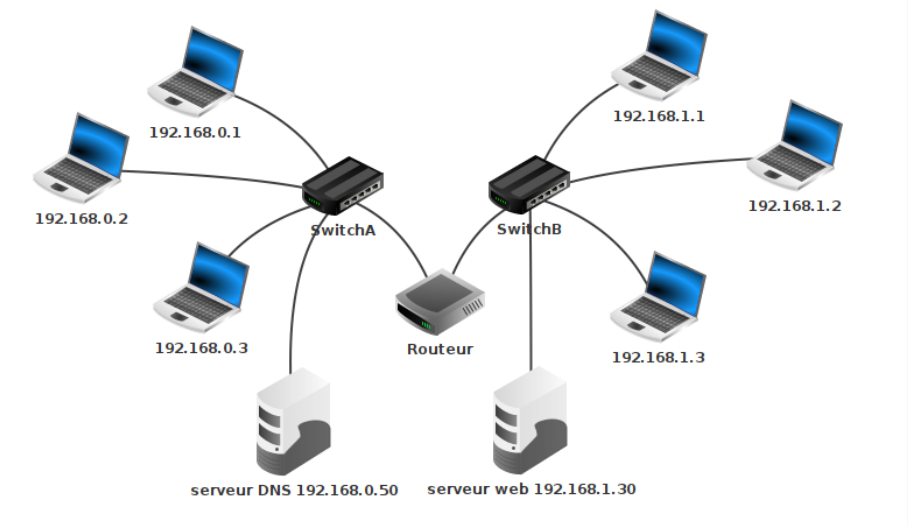
2. Démarrer le serveur web.
3. Ajouter un navigateur web sur la machine `192.168.0.1`.
4. Taper l'adresse IP du serveur web dans la barre d'adresse du navigateur.

Activité 6 : serveur DNS

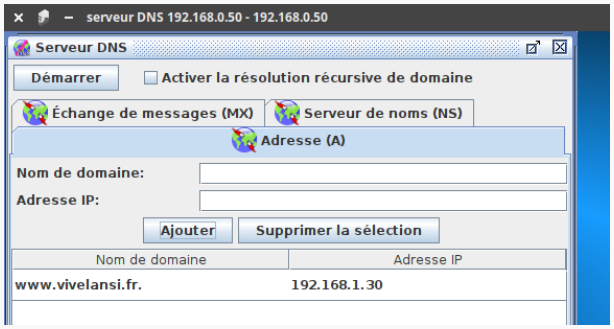
Lors d'une utilisation classique d'un navigateur web, c'est une url mémorisable qui s'affiche, et non une adresse IP : on retient en effet plus facilement `https://www.google.com/` que `http://216.58.213.131`, qui renvoient pourtant à la même adresse.

La machine qui assure ce rôle d'annuaire entre les serveurs web et leur adresse IP s'appelle un serveur DNS. Pour pouvoir indexer la totalité des sites internet, son rôle est structuré de manière hiérarchique.

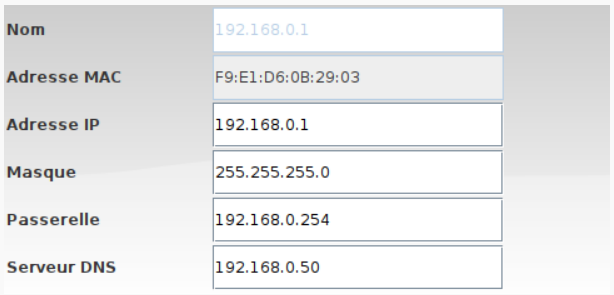
1. Ajouter un serveur DNS minimal, qui n'aura dans son annuaire qu'un seul site. Il faut pour cela raccorder une nouvelle machine (mais une machine déjà sur le réseau aurait très bien pu jouer ce rôle) et y installer un server DNS.



2. Sur ce serveur DNS, associer l'adresse `http://www.vivelansi.fr` à l'adresse IP `192.168.1.30`.



3. Sur la machine `192.168.0.1`, spécifier l'adresse du serveur DNS :



4. Dans la barre d'adresse du navigateur (de la machine `192.168.0.1`), essayer l'adresse `http://www.vivelansi.fr`.

3 Le modèle en couches

3.1 Découpage des données en paquets

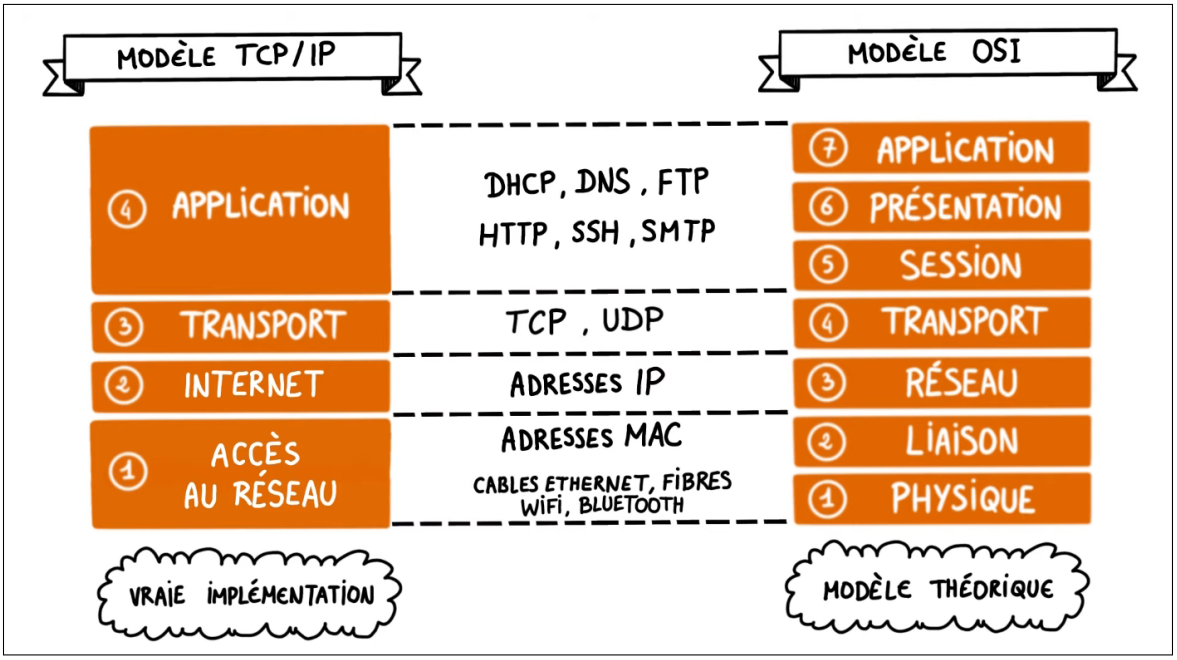
Dans un réseau informatique, si on veut transmettre une image de plusieurs mégaoctets, on n'envoie pas les données en un seul bloc mais on les découpe en paquets plus petits qui sont transmis séparément. Ainsi, il n'est pas nécessaire de tout retransmettre en cas d'erreur. De plus cela réduit les risques d'encombrement ou de blocage des liens.

3.2 Modèle en couches et encapsulation des données

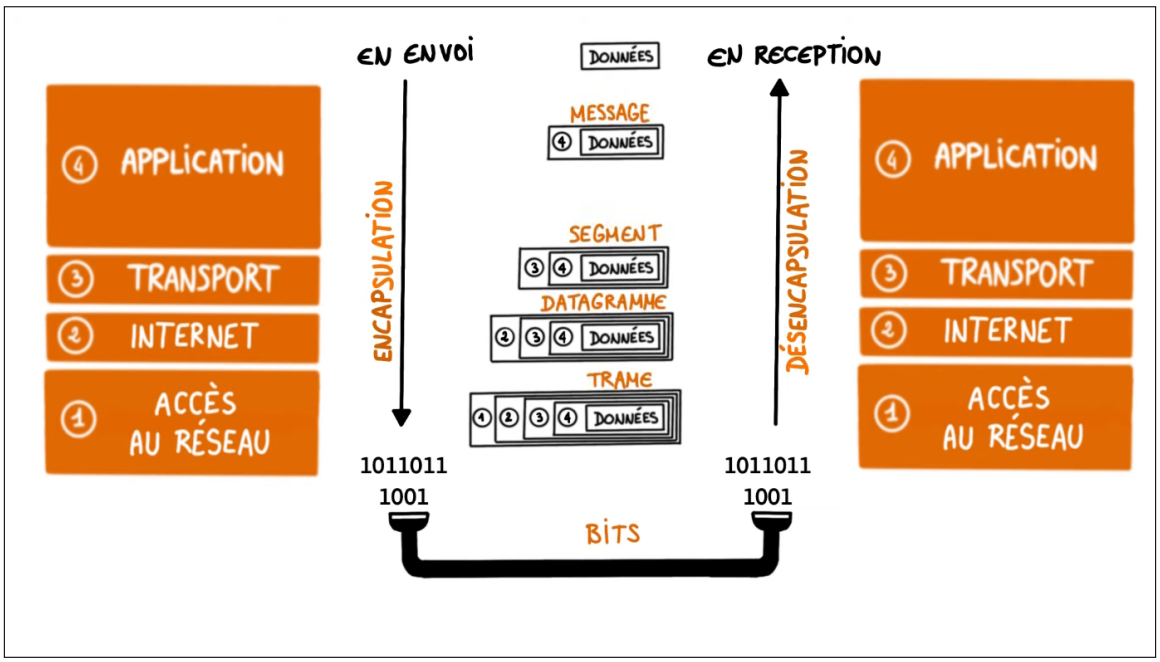
Exercice 5

1. Regarder la vidéo disponible ici.
2. Quel est le principe de l'encapsulation des données dans un réseau informatique ?
   (a) Cacher les données afin que l'on ne puisse pas les lire
   (b) Mettre les données les unes à la suite des autres
   (c) Inclure les données d'un protocole dans un autre protocole
   (d) Chiffrer les données afin que l'on ne puisse pas les lire

Les deux schémas suivants résument cette section :



Modèles TCP/IP et OSI



Encapsulation et désencapsulation dans le modèle TCP/IP

4 Protocole du bit alterné

Le protocole du bit alterné est un exemple simple de fiabilisation du transfert de données.

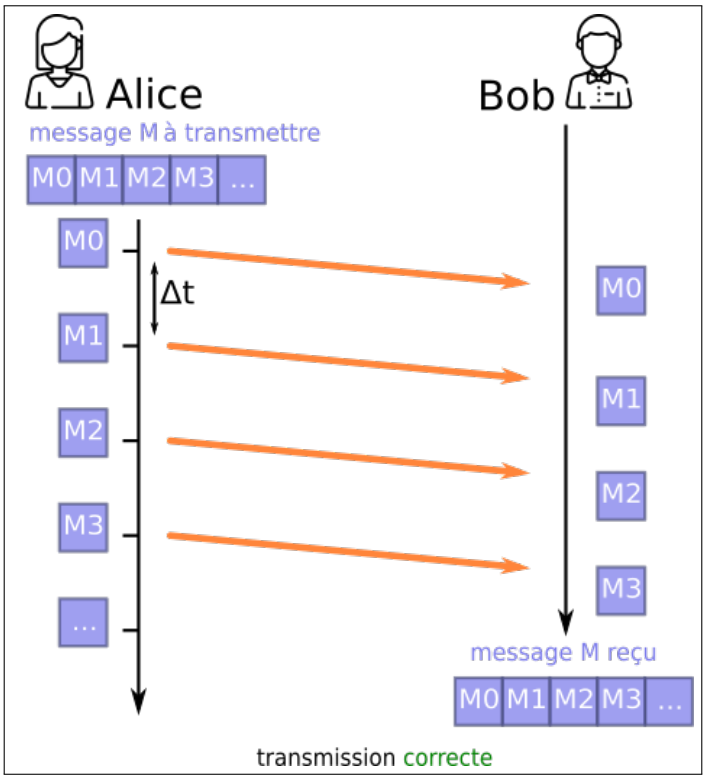
4.1 Contexte

— Alice veut envoyer à Bob un message `M`, qu'elle a prédécoupé en sous-messages `M0`, `M1`, `M2`, ...

— Alice envoie ses sous-messages à une cadence Δt fixée (en pratique, les sous-messages partent quand leur acquittement a été reçu ou qu'on a attendu celui-ci trop longtemps : on parle alors de timeout).

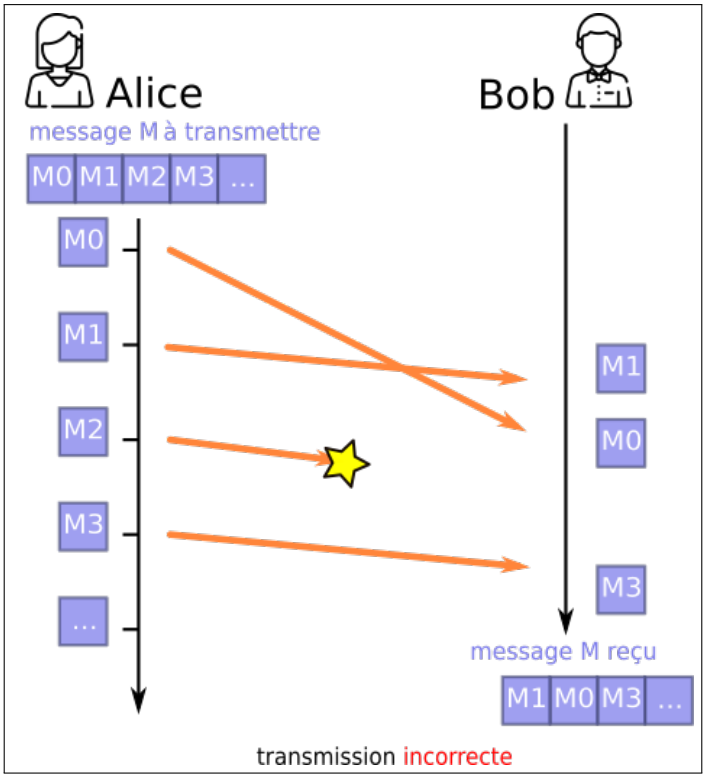
4.2 Situation idéale

Voici un schéma décrivant la situation idéale dans laquelle tous les sous-messages arrivent à destination, dans le bon ordre.



4.3 Situation réelle

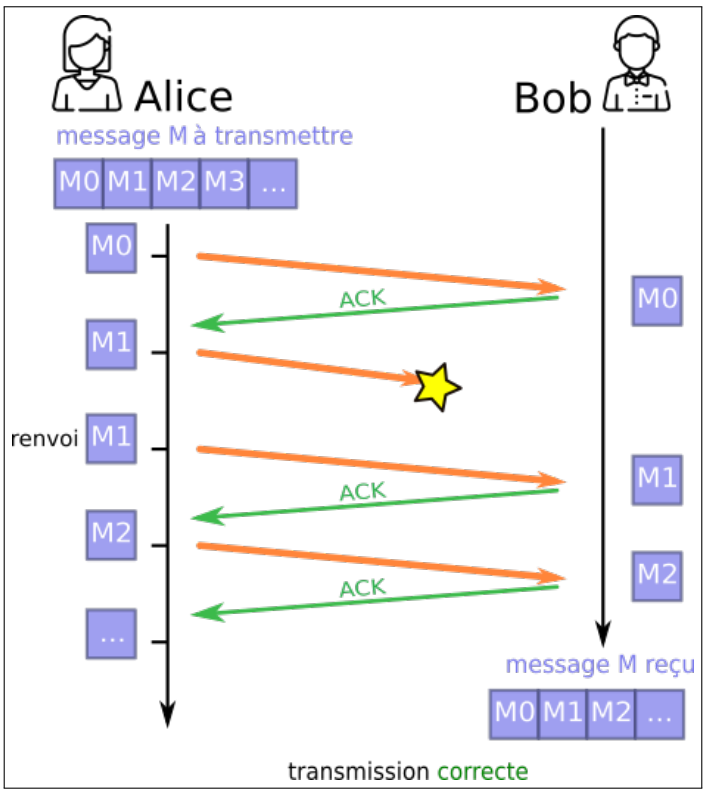
Mais parfois, les choses ne se passent pas toujours aussi bien car si on maîtrise parfaitement le timing de l'envoi des sous-messages d'Alice, on ne sait pas combien de temps vont mettre ces sous-messages pour arriver, ni même s'ils ne vont pas être détruits en route.



Le sous-message `M0` est arrivé après le `M1`, le message `M2` n'est jamais arrivé...
Numéroter les sous-messages afin que Bob puisse les remettre dans l'ordre ou redemander spécifiquement les sous-messages perdus est coûteux en ressources. Il existe une solution plus basique.

4.4 Idée naïve

Une idée naïve consiste de demander à Bob d'envoyer un signal pour dire à Alice qu'il vient bien de recevoir son sous-message. On appellera ce signal ACK (comme acknowledgement, traduisible par « accusé de réception »). Ce signal ACK permettra à Alice de renvoyer un message qu'elle considèrera comme perdu :

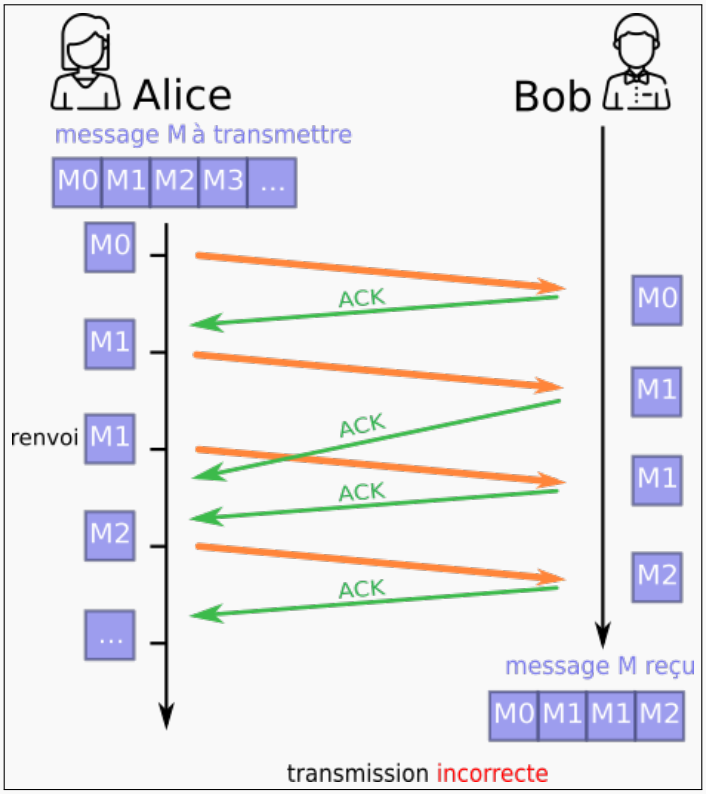


Exercice 6

Décrire la situation précédente.

Exercice 7

Expliquer pourquoi la solution décrite précédemment n'est pas suffisante à l'aide du schéma ci-dessous :



4.5 Protocole du bit alterné

Description du protocole

Bob va maintenant intégrer une méthode de validation du sous-message reçu. Il pourra décider de le garder ou de l'écarter. Le but est d'éviter les doublons.

Pour réaliser ceci, Alice va rajouter à chacun de ses sous-messages un bit de contrôle, qu'on appelera FLAG (drapeau). Au départ, ce FLAG vaut 0. Quand Bob reçoit un FLAG, il renvoie un ACK égal au FLAG reçu.

Alice va attendre cet ACK contenant le même bit que son dernier FLAG envoyé :

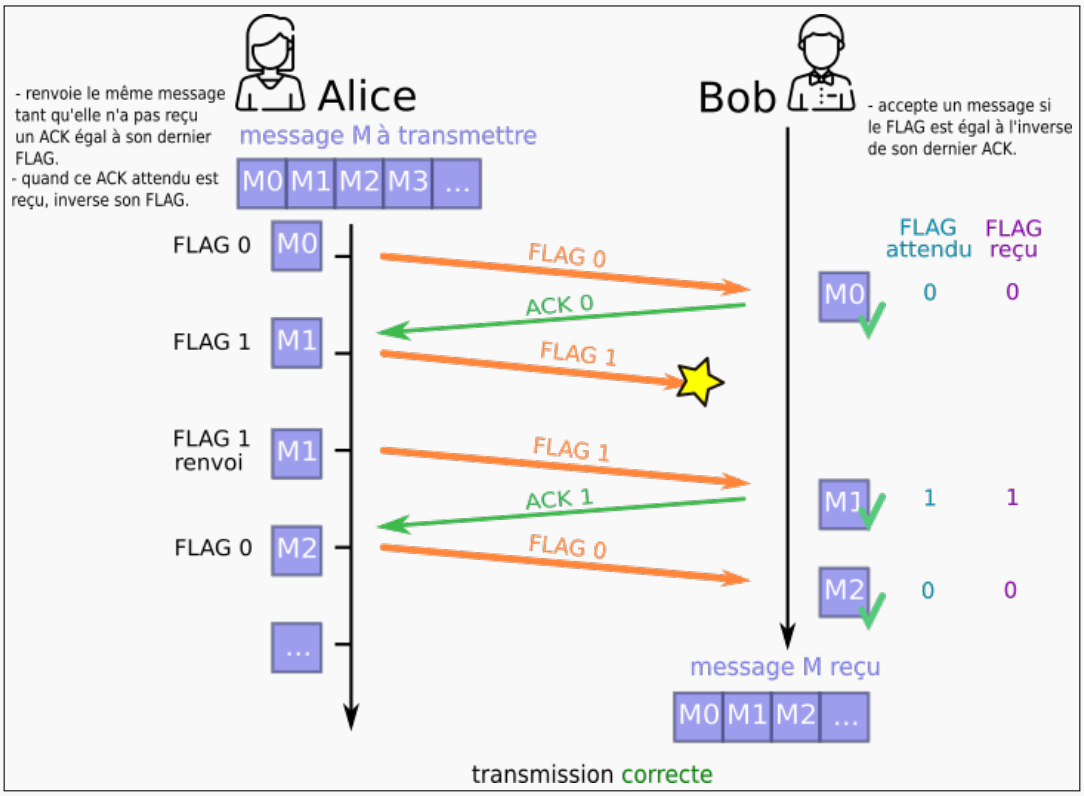
— tant qu'elle ne l'aura pas reçu, elle continuera à envoyer le même sous-message, avec le même FLAG ;

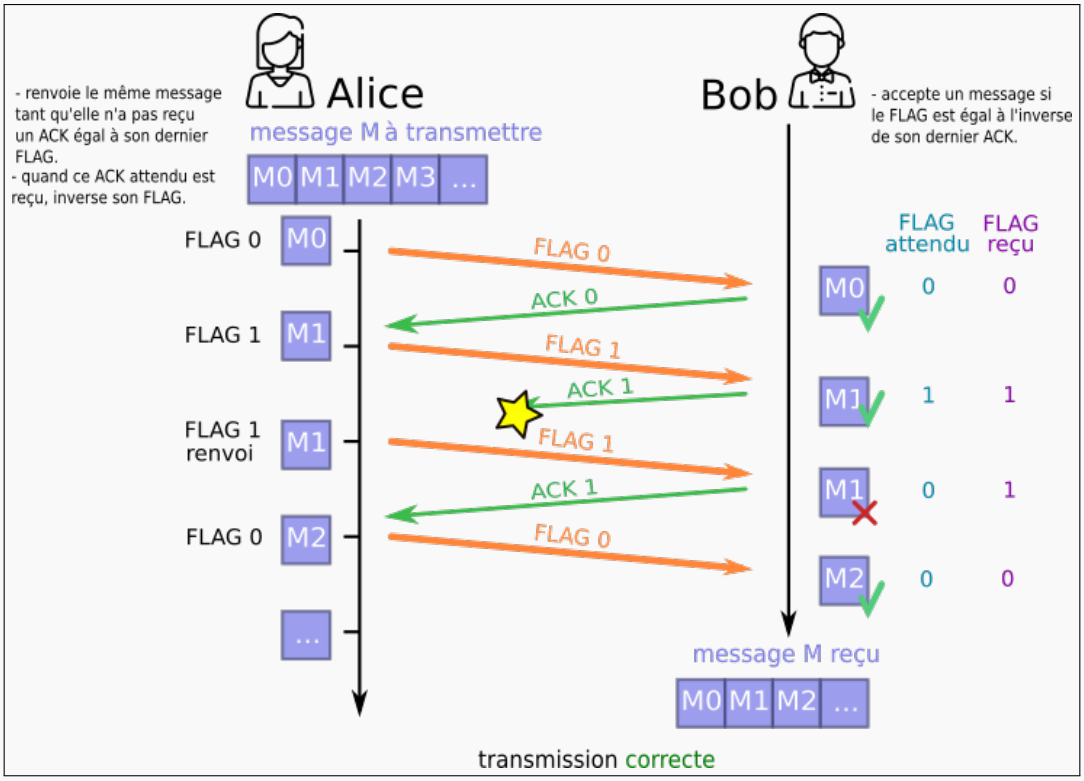
— dès qu'elle l'a reçu, elle peut envoyer un nouveau sous-message en inversant (« alternant ») le bit de son dernier FLAG (d'où le nom de ce protocole).

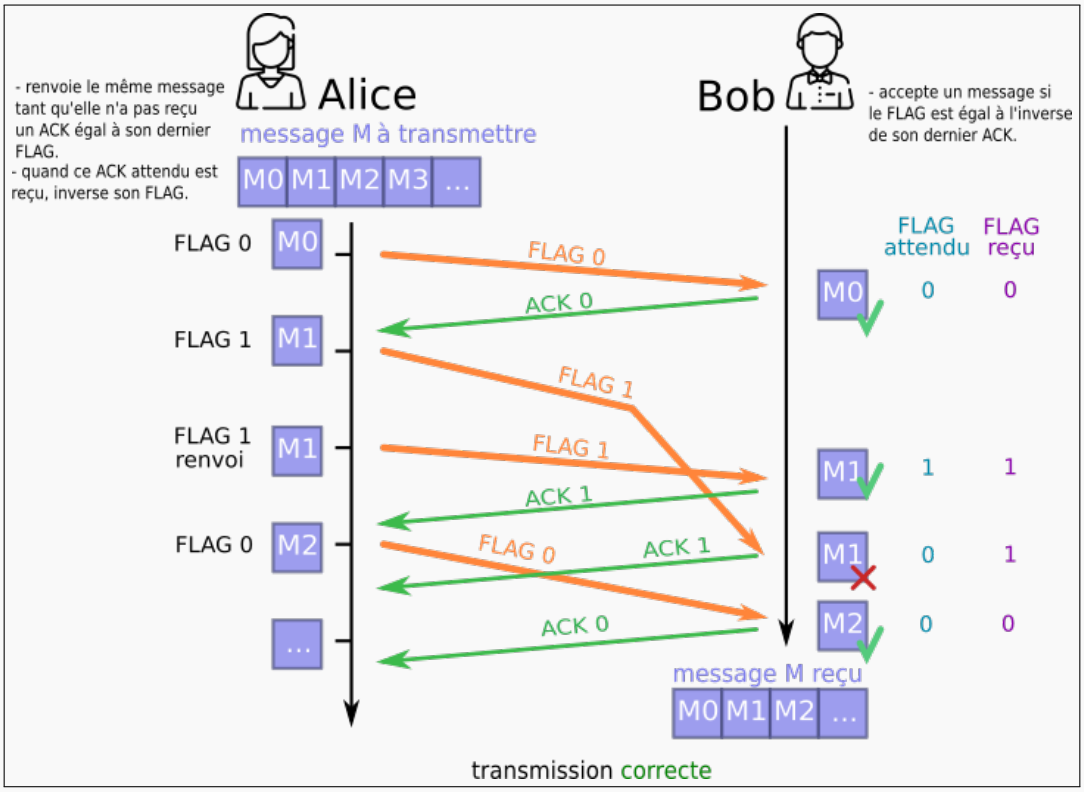
Bob, de son côté, va contrôler la validité de ce qu'il reçoit : il ne gardera que les sous-messages dont le FLAG est égal à l'inverse de son dernier ACK. C'est cette méthode qui lui permettra d'écarter les doublons.

Exercice 8

Observer le protocole du bit alterné dans les trois cas ci-dessous et expliquer pourquoi la transmission est correcte.







4.6 Conclusion

Le protocole du bit alterné a longtemps été utilisé au sein de la couche 2 du modèle OSI (distribution des trames Ethernet). Simple et léger, il peut toutefois être facilement mis en défaut, ce qui explique qu'il ait été remplacé par des protocoles plus performants.