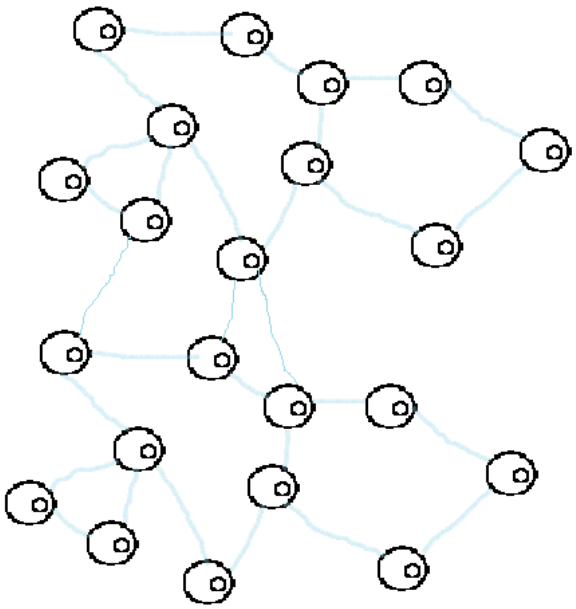
Activité 2 : Echanger des messages.

L'exercice demande de déplacer des chaises, les professeurs y sont habitués.

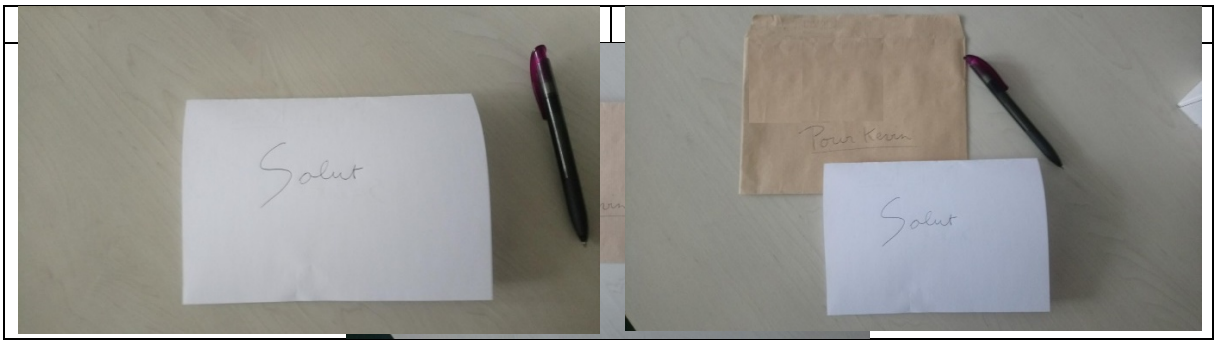
Chaque élève doit se placer où il veut à une longueur de bras minimum de chaque camarade. Il faut éviter de créer un grand cercle (anneau). Il peut y avoir plusieurs chemins pour aller au même endroit. En routage on appelle cela de la redondance.

Une fois les élèves en position :

Il faut leur expliquer qu'ils sont à présent des ordinateurs particuliers dotés de la capacité de transmettre des messages (de les router).
Toutefois ils ne peuvent envoyer une information (sous forme d'un petit mot) qu'à un voisin direct.



Demander à un élève (Farid) d'écrire un message à un camarade lointain (et éventuellement de le mettre dans une enveloppe).



Il ne peut le confier qu'à l'un de ses voisins directs.
Il est possible qu'il n'ait pas mis le destinataire (ce sera à exploiter)
Donc pour l'instant nous avons une enveloppe qui contient le message

En toute logique, l'enveloppe passe de main en main, la consigne est de ne jamais la renvoyer à

quelqu'un qui l'aurait déjà eu en main. Pour une meilleure visualisation, on peut demander aux élèves, par qui est passé le message, de se lever.
Il y a de fortes chances que du premier coup « Kévin » reçoive l'enveloppe.

Pour l'instant nous pouvons modéliser l'objet ainsi :

L'enveloppe	Message
Destinataire	Salut

Question : À la classe. Est-ce que Kévin a bien reçu le message ?

OUI

Imaginons que Kévin et Farid soient à une distance de 100 ou 1000 km l'un de l'autre.

Farid peut-il savoir si Kévin a bien eu le message ?

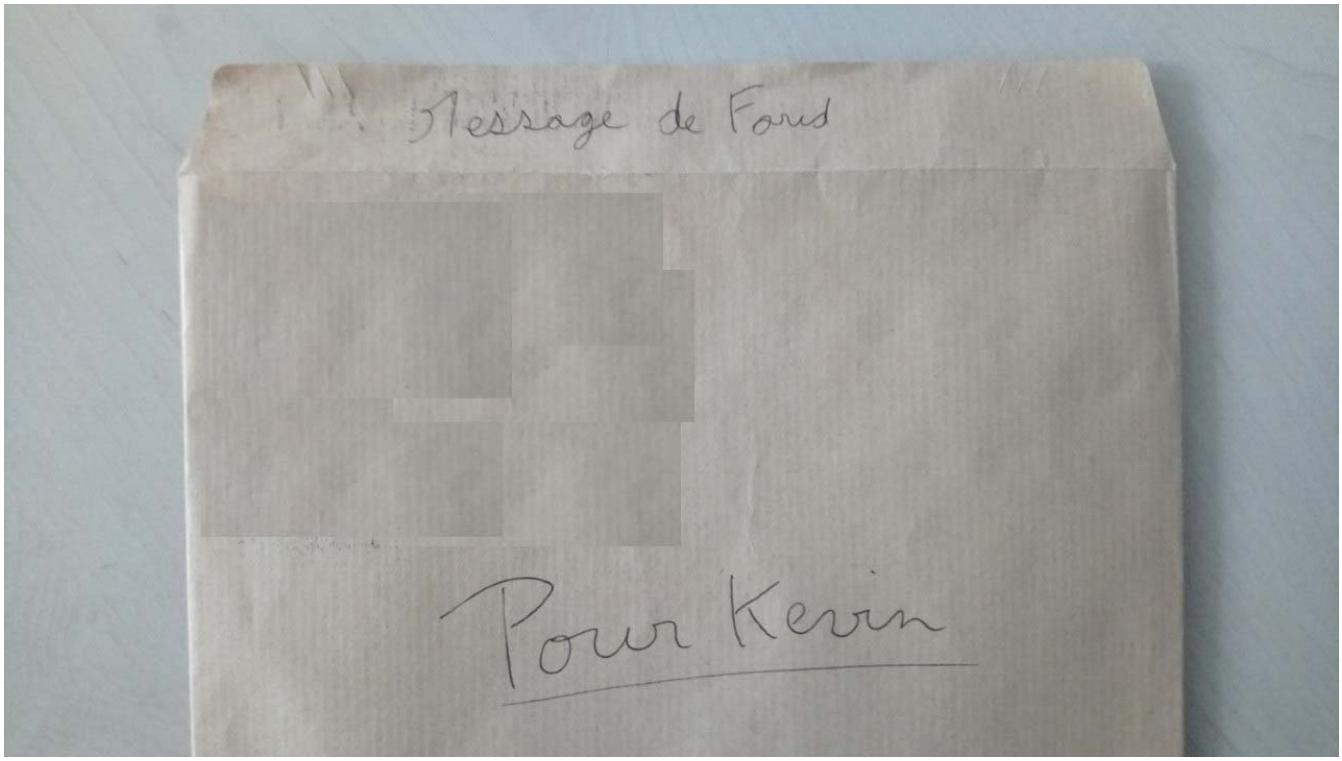
NON

COMMENT REMEDIER AU PROBLEME

Kévin doit accuser réception, dire qu'il a bien reçu le message.
C'est le mécanisme d'accusé de réception (acquittement, poignée de main, *acknowledgment*)

Oui mais comment va répondre Kévin ?

Il faut que Farid indique sur le message qu'il en est l'expéditeur.



Bilan et approfondissements :

Le message ne peut pas voyager seul, il lui faut un contenant avec des informations supplémentaires (expéditeur, destinataire, accusé de réception) pour s'assurer qu'il arrive à destination.

L'enveloppe Message

Destinataire	Expéditeur	Salut

En réseau informatique, on appelle cela un paquet et les informations supplémentaires sont normalisées dans les protocoles IP et TCP.

Entête IP	@IP SOURCE	@IP DESTINATION	Données IP/ Message

La seule différence, c'est que le paquet est transporté de manière électromagnétique et selon un code composé que de 0 et de 1 appelé bits (Binary digIT).

Par exemple 1000001 veut dire A et 1011010 veut dire Z. C'est le code Ascii[1].

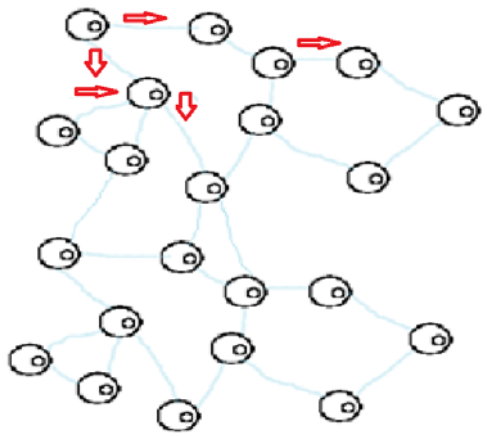
L'adresse IP est également transmise en binaire. Par souci de simplicité, on l'écrit souvent en « décimal pointé » x.x.x.x où x est compris entre 0 et 255. Ex : 172.31.0.1, 222.5.7.14. Ces adresses IP peuvent s'apparenter à un code postal : elles sont hiérarchiques et permettent de localiser le destinataire afin de lui envoyer des paquets.

Petit exercice pour aller plus loin sur les adresses IP en ANNEXE 2.

Activité 3 : Echangez des grands messages.

Le message est maintenant inscrit sur une feuille au format A4, trop grande pour être placée dans l'enveloppe (sans la plier). Idée des élèves (ou suggestion) : découper la feuille en morceaux plus petits qui tiennent dans l'enveloppe.

On met chaque morceau dans une nouvelle enveloppe et on relance le processus avec comme consigne aux participants de transmettre les enveloppes le plus rapidement possible, en utilisant notamment les divers chemins redondants à disposition.



On fera vite le constat qu'à l'arrivée on reçoit un *puzzle* qu'il est difficile de reconstituer.

[1] https://fr.wikipedia.org/wiki/American_Standard_Code_for_Information_Interchange

Question : Comment aider le destinataire à reconstituer l'information ? Numéroter les morceaux !

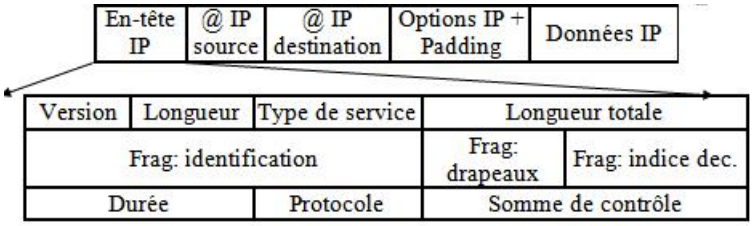
L'enveloppe Message

N°	Destinataire	Expéditeur	Morceau de la photo

Bilan et approfondissements :

Cette technique est utilisée par les protocoles TCP (création de segments...) et IP (fragmentation des paquets par certains routeurs) pour adapter les données aux capacités de transmission des réseaux physiques (MTU : Maximum Transmit Unit). Des champs spécifiques apparaissent dans les en-têtes IP et TCP.

Entête IP Avec N°	@IP SOURCE	@IP SOURCE	Fraction du message.



Activité 4 : réflexion sur la perte de paquets.

À ce moment de l'apprentissage, il est possible d'expliquer aux élèves que certains paquets peuvent se perdre où ne jamais arriver à destination (suite à la rupture d'un lien, mauvais routage...)

Question : Comment savez-vous qu'un paquet n'est jamais arrivé à destination ? Réponse attendue : la source n'a pas reçu d'accusé de réception.

Oui mais au bout de combien de temps considère-t-on un paquet perdu dans les protocoles TCP/IP ?

Question : Que feriez-vous si un élément n'arrive pas à destination (pas d'accusé de réception) ?

Réponse *attendue : renvoyer* le paquet

Question : Que devient un paquet qui se perd et qui ne trouve pas sa destination, est-ce qu'il ère à l'infini sur la toile ?

Bilan et approfondissements :

Dans le protocole TCP/IP, la durée au-delà de laquelle on considère que le paquet est perdu est appelée RTT[2] et est comprise entre 0 et 90 ms. C'est très court à échelle humaine mais tout va très vite dans un câble, donc 90ms est un temps assez long pour considérer un paquet perdu.

De plus, un paquet a une durée de vie TTL (Time To Live, 8 bits) : Ce champ est initialisé par l'émetteur puis diminué par chaque routeur traversé. Quand le TTL arrive à 0 (TTL de départ = 255 ou 127), le paquet est supprimé par le routeur qui avertit l'expéditeur (ex: principe de fonctionnement la commande *traceroute*).

Activité 5 : sécurité d'un message

Refaire le jeu de l'enveloppe. Demander à l'expéditeur d'envoyer un message personnel (quelque chose qui ne doit pas être connu par une tierce personne). Avant l'envoi, prévoir quelques complices sur le chemin de transmission dans le rôle de cyber-voyous (Hacker, Black-Hat: ils devront lire le message à haute voix s'il passe par eux).

Question : Comment faire pour éviter que l'information ne soit dévoilée ?

Réponse attendue : il faut *chiffrer* le message

Il est possible à ce moment-là de créer une séquence pour mettre en place des mécanismes ludiques de chiffrement (chiffre de César...).

Question : Est-il possible de faire des messages que seul le récepteur peut déchiffrer ?

OUI, s'il est le seul à disposer des informations pour le déchiffrer.

Il est possible d'évoquer les notions de chiffrement asymétriques, certificats... sans rentrer dans les détails

Pour aller plus loin:

Question : Pourquoi l'Etat a longtemps obligé les sociétés agréées fournissant des services de chiffrement sur le territoire français à procurer au service central de la sécurité des systèmes d'information les clés de chiffrement employées ?[3]

Les réponses doivent permettent aux élèves de comprendre grâce à une discussion qu'il est important qu'il y ait un régulateur. Sinon des personnes mal intentionnées pourraient en secret préparer des opérations illégales et dangereuses. Il faut préciser aussi que la grande majorité des conversations ne sont pas écoutées, c'est sous la direction d'un procureur et d'une enquête de police que se font les écoutes quand des indices permettent de suspecter des délits. La possibilité d'utiliser des mécanismes de chiffrement sans porte dérobée est encore en débat.

---

[2] https://fr.wikipedia.org/wiki/Transmission_Control_ProtocolRTT ou RTD (Round-Trip Time ou Round-Trip Delay) : Il s'agit du délai exprimé en ms du temps de réponse. Ce délai indique le temps mis par le paquet pour atteindre sa destination et revenir. Plus ce délai est proche de 0, au plus la qualité de la connexion est bonne

[3] https://fr.wikipedia.org/wiki/Chiffrement