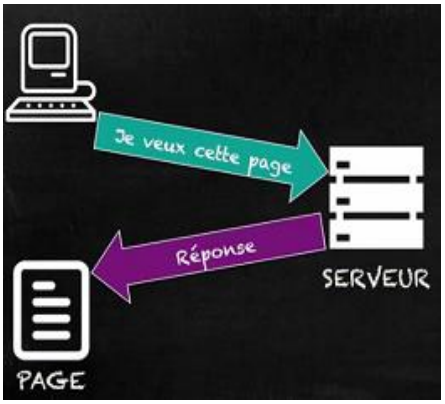
Nom : Prénom : Classe : Date :

Première Architecture-OS	Cours : Les réseaux informatiques	NSI

1. Le modèle de la boîte noire.

Quand on pense réseau, on pense à des enchevêtrements de câbles de toutes les couleurs, à des lumières qui clignotent,... Cela semble compliqué de relier ensemble tous ces éléments pour arriver à avoir des services tels que : surfer sur internet, regarder des vidéos en ligne ou téléphoner.



En fait, derrière cette complexité, il y a une structure cachée.

Pour qu'un réseau puisse fonctionner à grande échelle, il faut que les principes qui le constituent soient simples. Au lieu de voir le réseau comme un ensemble de câbles et d'équipements, nous allons essayer de le représenter plus simplement.

Quand nous surfons sur internet on tape le nom d'un serveur. Nous envoyons vers ce serveur un message disant «Je veux cette page ». Le serveur traite ce message et nous renvoie une réponse.

Nous allons considérer le réseau comme une « boîte noire ».

Ce qui va nous intéresser, ce sont les interactions entre nous et cette «boîte noire ». Comment les données font-elles pour passer d'un côté, puis de l'autre de la boîte ? Ce niveau d'abstraction peut également être suffisant pour les programmeurs qui développent des applications utilisant le réseau.

2. Notion de couche

Une voie de communication n'est jamais parfaite. Lors de la description du service postal, des erreurs peuvent se produire, les données sont organisées en paquets, le délai d'acheminement est variable, plusieurs destinataires peuvent exister derrière une même boite aux lettres…

Pour améliorer le service offert par un service de communication, donc des voies de communication qu'il fournit, un ensemble de règles sont définies et mise en œuvre. Ces règles sont appelées « protocole » de communication.

Nous appellerons « entité protocolaire » un composant logiciel ou matériel qui exécute ces règles. Une « entité protocolaire » met en œuvre un protocole particulier. Il existe dans les réseaux des centaines de protocoles différents.

Les règles qui définissent un protocole sont définies avec la plus grande précision dans des normes et standards internationaux.

L'assemblage d'un protocole et d'un service réseau forme un nouveau service réseau.

Il est donc possible par emboîtement de services et protocoles de construire autant de services qu'on le souhaite.

On parle aussi de couche protocolaire. Dans chaque équipement, une instance de l'entité protocolaire de cette couche doit être implantée.

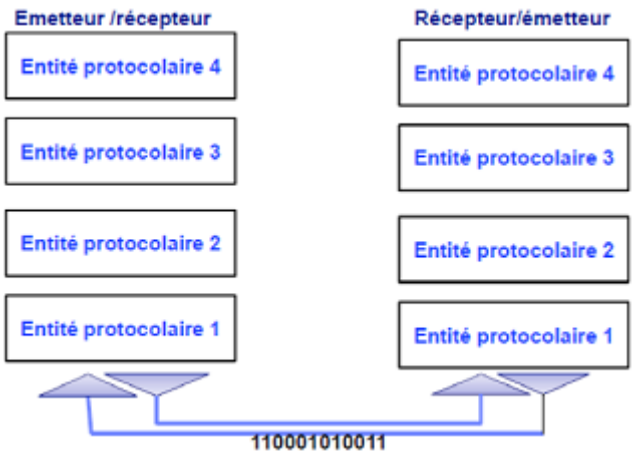


Figure 1 : Entité protocolaire

A la fin des années 70 l'ISO[1] a défini le modèle OSI[2], connu sou l'abréviation modèle ISO /OSI, qui sert aujourd'hui encore de référence dans la conception des réseaux de données.

[1] International Standard Organisation
[2] Open System Interconnexion

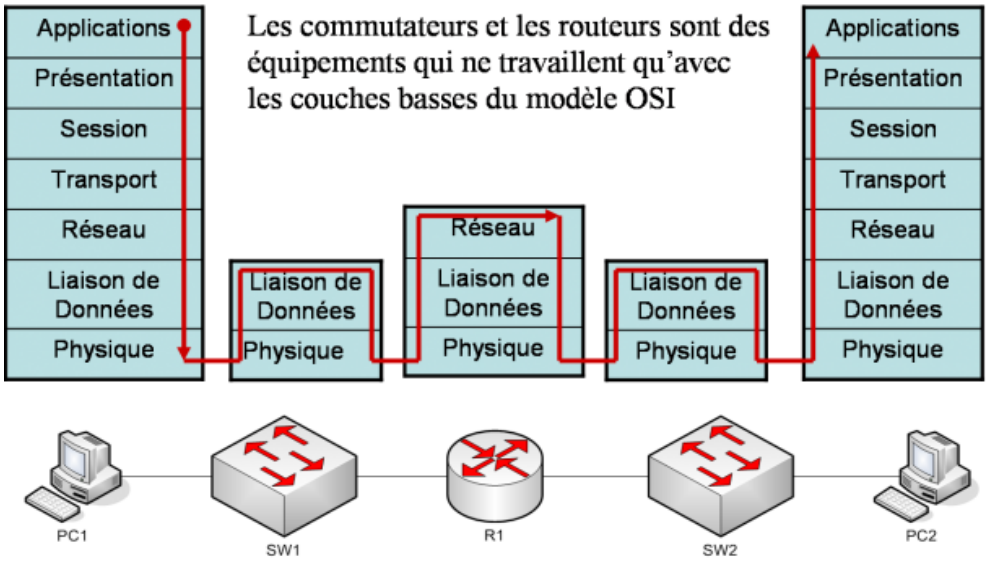
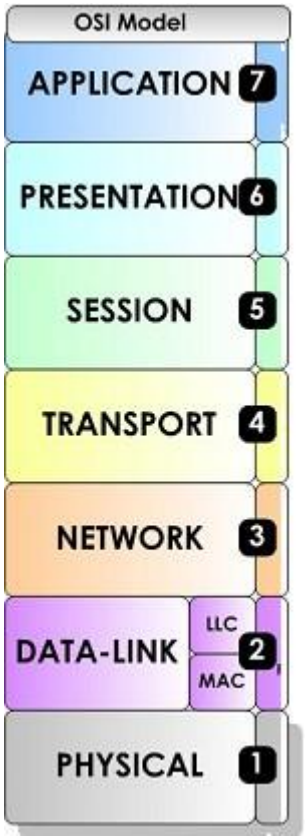


Figure 2 : modèle OSI/IOS

Ce modèle défini 7 couches. Au sein de chaque couche différentes normes et standards définissent les services fournis :



1. La couche physique définit les caractéristiques du support : métallique, optique, hertzien, micro-onde, la puissance et portée du signal, longueurs du câble, la forme des prises, le codage utilisé pour transmettre des bits sur le câble.
2. La couche liaison assure le transfert de l'information entre la machine et la voie physique. Elle détecte en général les erreurs et peut éventuellement mettre en œuvre des mécanismes de correction.
3. La couche réseau assure la fonction d'acheminement des messages à destination. Elle réalise le routage ou relayage ou commutation, des messages. Elle doit être capable de calculer et trouver les chemins. Pour cela, elle doit disposer de plusieurs liaisons avec les entités réseau voisines, jusqu'à atteindre la destination désirée.
4. La couche transport assure un transfert de données de manière transparente entre utilisateur en les déchargeant des détails d'exécution. Il existe de nombreux services de transport comme TCP et UDP.
5. La couche session a pour but de fournir des moyens de synchronisation. Elle est rarement implémentée au dessus du transport.
6. La couche présentation se charge de la représentation des informations que des entités d'application se communiquent. Elle est nécessaire du fait de la variété des représentations de données dans les différents systèmes.
7. La couche application contient différents protocoles dont les utilisateurs ont couramment besoin. HTTP[3], qui forme la base du World Wide Web, est un protocole d'application largement utilisé. Lorsqu'un navigateur veut afficher une page web, il transmet son nom au serveur qui l'héberge au moyen du protocole HTTP, et le serveur envoie la page en réponse. D'autres protocoles d'application sont utilisés pour le transfert de fichiers, le courrier électronique et les nouvelles (news).

3. Notion de protocole

Pour réaliser les règles définies par un protocole, les entités homologues ont besoin d'échanger des informations. Il y a au minimum les informations que l'utilisateur demande de transmettre que nous appellerons SDU pour Service Data Unit dans l'entité protocolaire.

[3]HyperText Transfer Protocol

L'objectif du service de communication est en général de délivrer la même donnée, le même SDU à destination. Donc ce qui rentre et sort aux extrémités d'une voie de communication est identique.

Pour réaliser le service de communication, les deux entités homologues vont s'échanger des messages que l'on appelle PDU pour Protocol Data Unit.

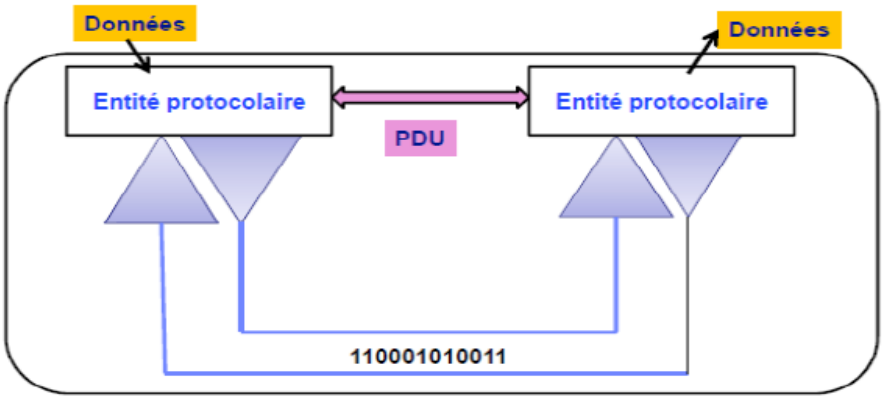


Figure 3 : Unité de Donnée Protocolaire

Ces PDU vont, en plus du contenu du SDU, contenir des informations dont le protocole a besoin pour construire les propriétés qu'il fournit. Ainsi, par exemple un protocole qui assure que les SDU seront délivrés dans le bon ordre introduira un numéro de séquence.

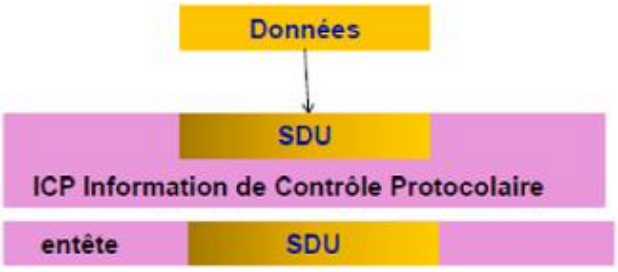
Un protocole qui assure que des SDU erronés ne sont pas délivrés introduira un code détection d'erreur.

Un protocole avec accusé de réception, qui comme le service du même nom à la poste veut pouvoir informer l'émetteur que le SDU est bien délivré introduira des PDU « accusés de réceptions ». Ces PDU circulent dans le sens inverse des données.

On appellera ICP, (Informations de Contrôle Protocolaire) toutes ces informations qui sont ajoutées par les entités protocolaires homologues. On parle aussi d'entête[4] car ces informations sont souvent placées avant le SDU dans le PDU. Il en est aussi souvent ajouté à la fin aussi, par exemple un code détecteur d'erreurs, on peut parler dans ce cas d'enqueue.

Il faut bien loger ces données supplémentaires. Elles vont donc s'ajouter au SDU. Si le PDU porte toutes les données du SDU, les données de protocole sont ajoutées. Si le PDU sert uniquement à la gestion du protocole, on parle de PDU de protocole.

On appelle souvent enveloppe ces informations de contrôle protocolaires que nous avons notées ICP. On dit aussi que les données sont encapsulées dans le PDU.



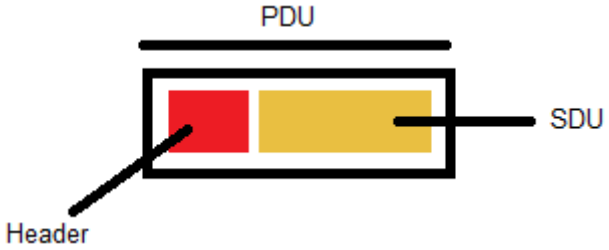


Figure 4 : constitution d'un PDU

Du coté de l'émetteur la donnée initiale est complétée, on dit aussi encapsulée, dans chaque entité protocolaire traversée, par des informations de contrôle protocolaire.

A l'inverse du coté du récepteur ces informations de contrôle protocolaire sont extraites et utilisées par le protocole. On dit que l'information utile est décapsulée pour être délivrée à la couche supérieure.

[4] header en anglais

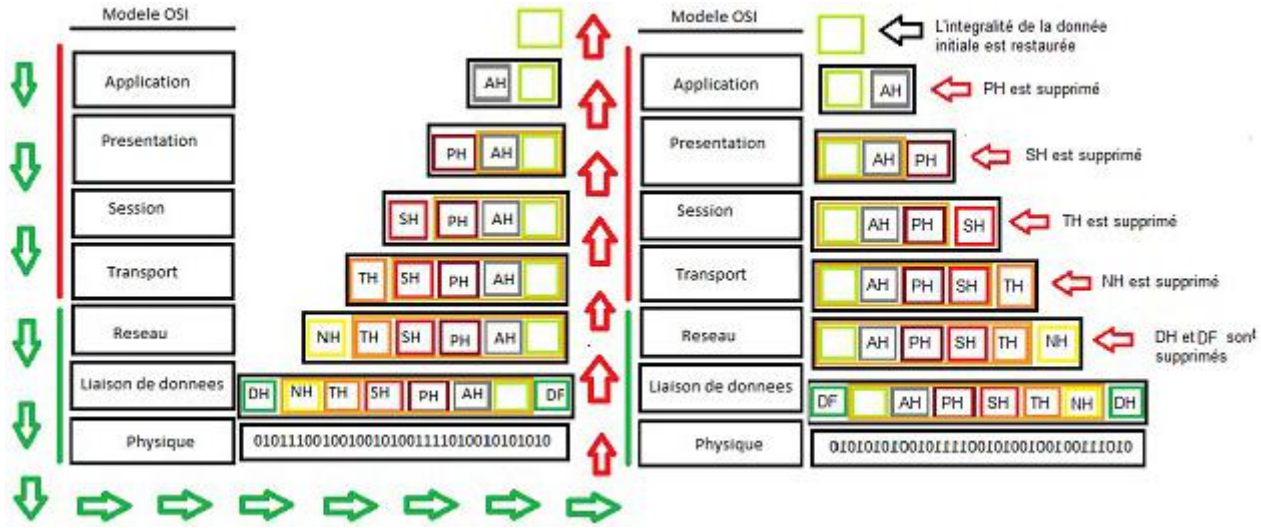


Figure 5 : encapsulation / décapsulation d'un SDU

4. Adressage IP

Un système de communication doit pouvoir permettre à n'importe quel hôte de se mettre en relation avec n'importe quel autre. Afin qu'il n'y ait pas d'ambiguïté pour la reconnaissance des hôtes possibles, il est absolument nécessaire d'admettre un principe général d'identification.

Lorsque l'on veut établir une communication, il est intuitivement indispensable de posséder trois informations :

1. Le nom de la machine distante,
2. son adresse,
3. la route à suivre pour y parvenir.

Le nom dit « qui » est l'hôte distant, l'adresse nous dit « où »' il se trouve et la route « comment » on y parvient.

Les adresses IP (version 4) sont standardisées sous forme d'un nombre de 32 bits qui permet à la fois l'identification de chaque hôte et du réseau auquel il appartient. Le choix des nombres composants une adresse IP n'est pas laissé au hasard, au contraire il fait l'objet d'une attention particulière notamment pour faciliter les opérations de routage.

4.1. Anatomie d'une adresse IP

Une adresse IP (version 4) est un nombre de 4 octets (32 bits) que l'on a coutume de représenter sous une forme décimale pointée : 4 entiers allant de 0 à 255, séparés par des points.

Chaque adresse IP contient donc deux informations basiques, une adresse de réseau et une adresse d'hôte. La combinaison des deux désigne de manière unique une machine et une seule sur l'Internet.

La partie réseau (NetID) de l'adresse IP vient toujours en tête, la partie hôte (HostID) est donc toujours en queue.

Exemple :	Réseau	Réseau	Réseau	Machine

Prenons l'exemple d'une machine dont l'adresse serait 131.254.100.48. Si les trois premiers octets désignent l'adresse du réseau, toutes les machines de ce réseau auront une adresse commençant par 131.254.100.xxx.

On appelle cette partie de l'adresse le préfixe du réseau.

Dans notre exemple, il a une longueur de 24 bits. On indique sa taille à la suite de l'adresse IPv4 : dans notre exemple la machine aura l'adresse suivante : 131.254.100.48 /24.

Les 24 premiers bits désignent le préfixe du réseau :

10000011.11111110.01100100.xxxxxxxx

Cela veut dire que l'identification de l'interface réseau de la machine comprend 8 bits, on peut donc avoir 2^8 = 256 possibilités soit 256 machines différentes dans le réseau.

Le préfixe du réseau peut être facilement retrouvé en multipliant l'adresse de la machine par un netmask ou masque du réseau. Si n est la longueur du préfixe, le masque de réseau est constitué de 32 bits dont les n premiers sont des 1 et les suivants sont à 0.

Reprenons l'exemple : l'adresse 131.254.100.48 /24 indique que le préfixe a une longueur de 24 bits. Le masque de réseau comportera donc 24 bits à 1 suivis de 8 bits à 0 :

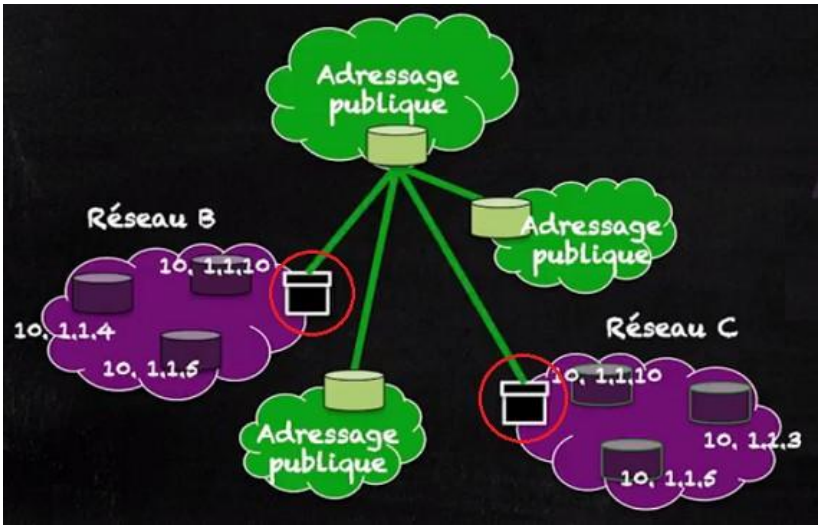
11111111111111111111111100000000

Soit 255.255.255.0 En multipliant le masque de réseau par l'adresse IP, on peut isoler le préfixe du réseau.

4.2. Adresses publiques ou privées

La forte croissance du nombre de machines connectées à l'Internet conduit à l'épuisement des adresses IPv4.

Une des mesures d'urgence prises est le recours à l'adressage privé. Les adresses IPv4 peuvent être publiques ou privées. Les adresses publiques permettent à une machine de communiquer avec l'Internet en désignant de façon unique cette machine ou une interface réseau dans l'Internet.



Les adresses privées peuvent être attribuées dans des réseaux internes qui n'ont pas vocation à communiquer directement avec Internet.

Les adresses privées peuvent être présentes dans plusieurs réseaux et ne peuvent donc pas être distinguées dans l'Internet. On dit que les adresses privées ne sont pas routables.

Si un réseau utilisant un adressage privé veut communiquer avec l'Internet, il faudra qu'un équipement fasse une translation (ou traduction) entre l'adresse privée et une adresse publique qui serait disponible pour dialoguer avec l'Internet. On appelle cette opération le NAT[5].

5. La couche transport

5.1. Le transport de bout-en bout

Une application désirant communiquer avec une autre application distante va demander au système d'exploitation qui l'héberge d'ouvrir ce canal de communication à destination de la machine qui accueille l'application réceptrice. Le système d'exploitation va alors se charger de contacter cette machine, identifiée par son adresse IP et d'ouvrir ce canal de communication sur lequel les applications pourront alors échanger des données.

Pour permettre à plusieurs applications de coexister sur la même machine, la couche transport introduit un niveau d'adressage supplémentaire qu'on appelle le numéro de port. Le numéro de port est un simple numéro, sur 16 bits, qui vient s'ajouter à l'adresse IP, permettant ainsi d'identifier une application fonctionnant sur une machine.

Le système d'exploitation va allouer à une application un ou plusieurs numéros de port de façon exclusive. Aucune autre application ne pourra utiliser le même numéro de port au même moment.

Une application serveur, dont le fonctionnement classique est d'attendre les connexions des applications clientes, va réserver son ou ses numéros de port au moment de son lancement. Une application cliente, dont le fonctionnement est plus dynamique, va réserver son numéro de port au moment où elle fera la demande de connexion vers le serveur distant qu'elle cherche à joindre.

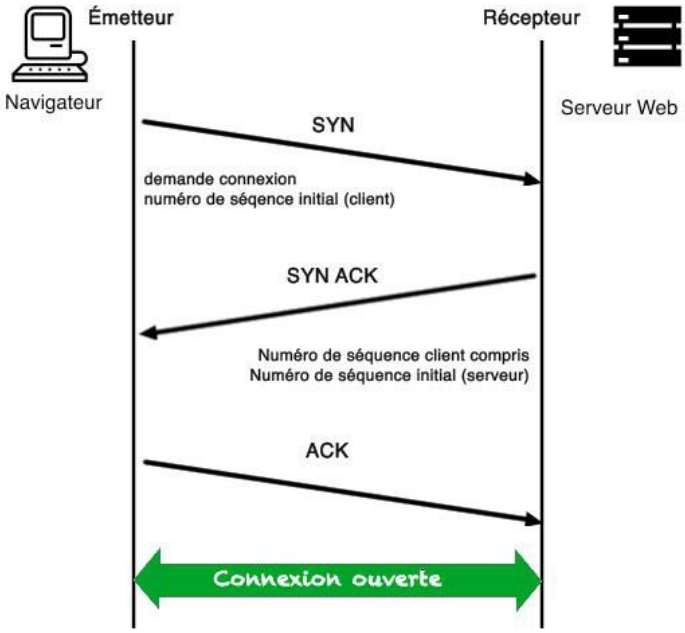
[5]Network Address Translation : Traduction d'adresse réseau

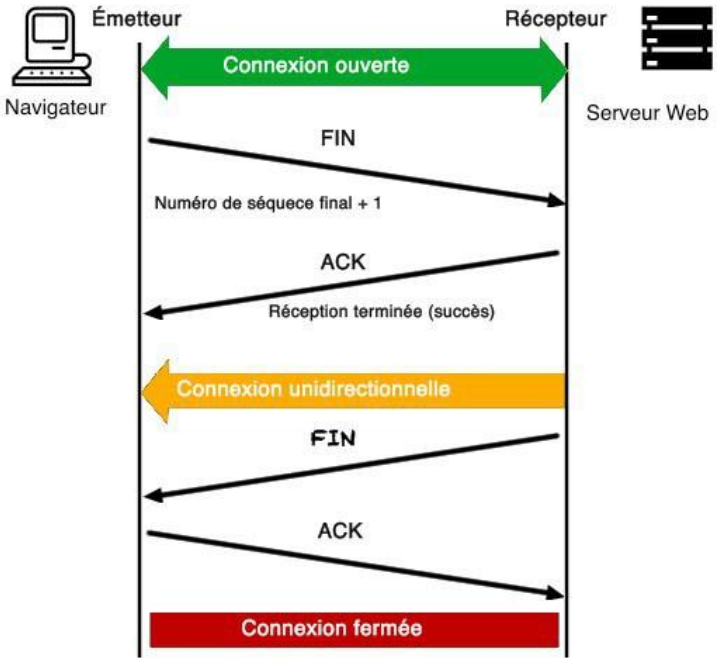
Les numéros de port de 0 à 1023 sont généralement utilisés pour les applications très largement répandues telles que les serveurs web, les serveurs FTP[6], les serveurs e-mail, etc. Les numéros de port de 1024 à 49151 sont destinés à des applications qui possèdent une, deux ou assez peu d'implémentations et sont déclarées en général auprès d'un organisme central qui s'appelle l'IANA[7]. Les numéros de port de 49152 à 65535 sont réservés à l'usage privé et sont en général utilisés pour recevoir les réponses aux requêtes que l'on envoie.

5.2. Session TCP : démarrer et terminer un dialogue

TCP utilise les acquittements pour s'assurer de la bonne réception des segments. Un émetteur envoie dans le réseau une séquence de segments et reçoit en retour une séquence d'acquittements. Cependant les segments comme les acquittements sont des paquets IP qui transitent dans le réseau. Ils peuvent donc être retardés et rien ne garantit que l'ordre dans lequel les acquittements seront reçus corresponde bien à l'ordre dans lequel les segments ont été envoyés.

La phase d'ouverture de connexion est composée de 3 messages. Le premier message, appelé synchronisation, est émis par l'initiateur de la connexion. Prenons l'exemple du dialogue entre un navigateur web et un serveur. Le navigateur démarre cet échange en émettant ce message de synchronisation dans lequel il inclura son numéro de séquence initial. Le serveur lui répondra en acquittant la réception de ce numéro de séquence et en incluant dans ce message d'acquittement son propre numéro de séquence initial. En effet, une connexion TCP est toujours ouverte dans les 2 sens et les deux flux de données sont, du point de vue de TCP, indépendants. Leurs numéros de séquence ne sont donc pas alignés. À la réception de ce 2ème message, le navigateur renverra au serveur un dernier acquittement et l'échange pourra alors commencer.





Une fois que le navigateur a terminé la transmission de ses données, il envoie au serveur un message de fin. Ce message contient le dernier numéro de séquence des données plus un. À la réception de ce message, le serveur peut vérifier qu'il a bien reçu l'intégralité des données et, le cas échéant, enverra au navigateur un message d'acquittement. La connexion est alors fermée dans le sens navigateur vers serveur. Elle reste cependant ouverte dans le sens serveur vers navigateur et devra être fermée de manière analogue à l'initiative du serveur.

[6] File Transfert Protocol
[7] Internet Assigned Numbers Authority