Protocoles de communication dans un réseau

1. Plusieurs niveaux d'interaction, modèle en couche

Les échanges entre deux machines s'effectuent à plusieurs niveaux d'interaction, sur plusieurs couches.

Exemple d'une requête HTTP dans le modèle TCP/IP

- Couche application, que l'on peut aussi découper en plusieurs niveaux :
  - l'utilisateur clique sur un lien, le serveur renvoie une page web
  - le client envoie un message contenant une URL, le serveur renvoie un message contenant un fichier HTML
- Couche transport : le message du client est découpé en paquets
- Couche internet : les différents routeurs du réseau les acheminent vers le serveur (ou le client au retour)
- Couche accès réseau : pour envoyer les paquets, chaque bit (0 ou 1) est transmis comme un signal électrique sur une ligne.

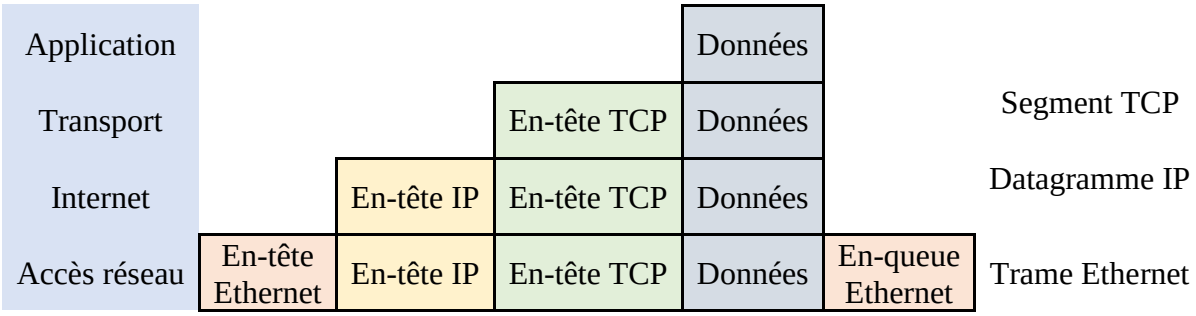
Chaque niveau utilise les fonctions du niveau inférieur.
Chaque couche dispose de ses protocoles de communication.

Couche du modèle TCP/IP	Principaux protocoles de communication	Niveau
Application	HTTP FTP SMTP POP3 IMAP DNS Telnet SSH …	Application
Transport	TCP UDP …	Système d'exploitation
Internet	IP ICMP ARP DHCP …	
Accès réseau	ETHERNET WIFI …	Carte réseau

Dans le modèle OSI, les échanges sont découpés en sept couches.
https://fr.wikipedia.org/wiki/Mod%C3%A8le_OSI

2. Découpage des données en paquets et encapsulation

Les données à transmettre sont découpées en paquets qui sont encapsulées suivant les différents protocoles.



3. Principaux protocoles de communication

Un protocole de communication définit plusieurs règles pour communiquer sur une même couche d'abstraction entre deux machines.

3.1. Couches transport et internet

3.1.1. IP - Internet Protocol

Le protocole IP assure l'acheminement des paquets (datagrammes) à destination rapidement sans se préoccuper de leur contenu et sans aucune garantie de résultat. C'est un protocole non fiable : les paquets peuvent être corrompus, perdus, dupliqués, désordonnées … Les paquets peuvent passer par des chemins différents, chaque routeur décidant du chemin à suivre en prenant en compte l'état du réseau en temps réel.

3.1.2. TCP – Transmission Control Protocol

Le protocole TCP complète le protocole IP en assurant la fiabilité du transport des paquets. Il est beaucoup plus complexe qu'IP. Il initialise et met fin à la connexion, et s'assure de l'intégrité des paquets, renvoie les paquets perdus ou corrompus et les remet dans l'ordre d'émission. Il gère aussi la congestion réseau, en freinant les gros serveurs si les petits saturent. TCP effectue son traitement aux extrémités du trajet.
TCP envoie une salve de paquets et les garde dans une petite mémoire. Il attend ensuite les acquittements (accusés de réception). S'il ne reçoit pas de réponse au bout de quelques secondes, il renvoie le paquet. Dès qu'il reçoit un acquittement (du type « tous les paquets jusqu'au 5 sont bien arrivés »), il libère la place correspondante dans la mémoire pour pouvoir y mettre des nouveaux paquets qu'il envoie.

3.1.3. UDP – User Datagram Protocol

UDP est un protocole cousin de TCP beaucoup plus simple. Il ne se soucie pas que le paquet arrive bien, mais est beaucoup plus réactif. On l'utilise par exemple dans le streaming ou les jeux vidéo. Une erreur de transmission pourra causer un petit défaut d'affichage mais on privilégie la réactivité.

3.1.4. Autres protocoles

ICMP, Internet Control Message Protocol, accompagne IP pour transporter des messages de contrôle et d'erreur lorsqu'un hôte est inaccessible par exemple.

DHCP, Dynamic Host Configuration Protocol, permet à un ordinateur qui se connecte sur un réseau d'obtenir automatiquement sa configuration, principalement son adresse IP.

ARP, Address Resolution Protocol, fait le lien entre l'adresse IP et l'adresse MAC d'une machine. Dans un réseau, les machines sont identifiées par leurs adresses physique MAC unique au monde. Lors d'un changement de carte réseau, l'adresse MAC de la machine change mais pas son adresse IP.

3.2. Couches accès réseau

Ethernet est le protocole le plus utilisé dans les réseaux filaires (câbles de cuivre ou fibres optiques).
Le **Wi-Fi** est un protocole utilisé dans les réseaux sans fils. Les protocoles Ethernet et Wi-Fi sont définis par les normes IEEE 802 (Institute of Electrical and Electronics Engineers).

3.3. Couches application

DNS, Domain Name System, est le protocole utilisé pour traduire les noms de domaine internet en adresse IP. Ainsi, nslookup www.qwant.com renvoie l'adresse IP 194.187.168.99. L'adresse renvoyée ne fonctionne pas toujours car elle peut correspondre à une machine faisant tourner plusieurs machines virtuelles.
Le protocole DNS n'a jamais été modifié depuis sa création en 1983, ce qui pose des problèmes de sécurité. On essaie actuellement de le mettre à jour. Il y a 13 serveurs DNS dans le monde. Les requêtes DNS sont transmises par UDP, ce qui nécessite 2 paquets par requête. TCP nécessiterait 4 paquets (ouverture et fermeture en plus de la requête et la réponse).

IMAP, Interactive Message Access Protocol et **POP3**, Post Office Protocol 3, sont les protocoles permettant de récupérer les courriers électroniques. **SMTP**, Simple Mail Transfer Protocol gère leur envoi.

FTP, File Transfert Protocol est utilisé pour le transfert de fichier.

Les protocoles **Telnet** et **SSH** gèrent l'accès à une machine distante.

HTTP, HyperText Transfert Protocol, ou HTTPS pour la version sécurisée, est le protocole de transfert des pages HTML permettant de naviguer sur le Web. Le client envoie la requête HTTP au serveur. Le serveur renvoie la réponse, par exemple une page HTML.
Les principales requêtes HTTP sont GET pour demander une ressource au serveur (une page web, une image…) et POST pour ajouter une ressource au serveur (un message dans un forum per exemple).

Exemple d'échanges
On entre un nom de domaine dans un navigateur. Le protocole DNS demande et récupère l'adresse IP via UDP (deux paquets).
TCP initialise ensuite la connexion entre le client et le serveur via trois paquets (requête SYN pour la demande de synchronisation, acquittement du serveur SYN-ACK, puis du client ACK).
HTTP envoie la requête GET via TCP (deux paquets, envoi, acquittement), puis deux paquets HTTP contenant la page HTML envoyée par le serveur (réception, acquittement).
Toute ressource qui n'est pas contenue dans la page (image, feuille de style, …) requiert une requête GET supplémentaire (et donc au moins quatre paquets).
Les trois dernières requêtes FIN, FIN-ACK, ACK ferment la connexion TCP.

4. Adresses IP, ports et sockets

IPv4/IPv6
Le protocole IPv4 utilisent des adresses 32 bits et il n'y a plus assez d'adresses possibles. Il est remplacé par IPv6, sur 128 bits. Les machines intérieures à notre réseau sont toutes visibles de l'extérieur en IPv6 alors qu'en IPv4, elles sont cachées derrière la box.
ip addr sous Linux ou ipconfig sous Windows renvoie les deux adresses IPv4 et IPv6. L'IPv6 a deux adresses, une publique et une pour communiquer avec les membres du réseau.

Ports et sockets
L'adresse de transport est constituée de l'adresse IP et du numéro de port sur 16 bits.
Les ports permettent un multiplexage de connexions (faire passer plusieurs connexions par le même support de transmission). Les ports inférieurs à 1024 sont appelés ports réservés. Parmi les plus utilisés, on trouve :

- 21 → FTP
- 25 → SMTP
- 80 → HTTP
- 110 → POP
- 143 → IMAP
- 443 → HTTPS

Une connexion client/serveur est identifiée par un quadruplé unique pour chaque connexion appelé **socket** :

(ip_src, port_src, ip_dest, port_dest)

Le terme socket désigne aussi les bibliothèques logicielles gérant l'accès au réseau (import socket en Python).

Firefox a un port par onglet. Ainsi, si on lance plusieurs connexions au même site, le site utilise toujours le même port, mais chaque connexion est identifiée de manière unique puisqu'on a un port différent par onglet.

La commande netstat renvoie la liste des connexions actives sous Windows et sous Linux.

5. Protocole du bit alterné

Lors des transferts de trames Ethernet (couche accès réseau), l'émetteur envoie une trame et attend l’acquittement du récepteur avant d'envoyer la suivante. Si l'émetteur ne reçoit pas un acquittement passé un certain délai (timeout), il considère la trame perdue et la renvoie. Ce système crée des doublons.

Le protocole du bit alterné consiste à numéroter les trames 0 ou 1, en alternance. Le récepteur rejette les trames qui ne correspondent pas au numéro attendu. Ainsi, si un doublon arrive, il va être rejeté.