HELLO Valentin

LEFORT Enzo

Les protocoles TCP et UDP

Le protocole TCP

TCP est un protocole orienté connexion de bout en bout fiable qui assure la transmission des données. Certaines des principales fonctions de TCP incluent la détection d'erreur, le démarrage lent, le contrôle de flux et le contrôle de la congestion. TCP est un mécanisme de transmission fiable. Exemples typiques d'applications TCP et de numéros de port: port de données FTP (20), port de contrôle FTP (21), SSH (222), Telnet (23), DNS (53), HTTP (80) et HTTPS (443).

Le logiciel TCP est contrôlé par diverses applications réseau (telles que des navigateurs Web ou des serveurs) via des interfaces spécifiques. Chaque connexion doit toujours être identifiée par deux points clairement définis (client et serveur). Le rôle du client et le rôle du serveur n'ont aucune importance. L'important est que pour chacun de ces points, le logiciel TCP dispose d'une paire ordonnée comprenant l'adresse IP et le port

Les avantages du TCP :

Il est fiable car la réception et la confirmation du paquet sont assurées. Il oblige le terminal à établir un canal sécurisé avant d'envoyer un message. Aucun colis ne sera endommagé ou perdu pendant le transport, ce qui signifie que vous recevrez le contenu que vous avez demandé.

Les inconvénients du TCP :

Il est connu pour ses performances médiocres sur les réseaux sans fil. C'est dû au fait que les liaisons sans fil ont tendance à rejeter les paquets de données pendant la transmission en raison du « bruit » sur le canal radio. Puisqu'il a besoin d'un ensemble complet de paquets de données pour transmettre des messages, il provoquera un court délai de transmission dans le processus de perte de paquets de données, ce qui conduit à un temps d'attente plus long pour le chargement et un temps de retard rapide.

Différence avec le protocole UDP :

TCP permet au système de contrôler la livraison des paquets de données de deux manières. Tout d'abord, TCP numérote chaque paquet afin que le point de terminaison cible les renvoie dans le bon ordre. Deuxièmement, TCP contient des mécanismes pour garantir que le point final cible reçoit chaque paquet.

Après avoir reçu le paquet de données, le dispositif récepteur envoie un message à l'expéditeur pour confirmer que la livraison a été reçue. Si l'expéditeur ne reçoit pas de réponse du récepteur, l'expéditeur retransmettra le paquet de données jusqu'à ce que le point d'extrémité reçoive avec succès le paquet de données ou annule la communication. TCP comprend également des fonctions de vérification des erreurs pour garantir qu'aucune donnée n'est corrompue.

Le protocole UDP

Le User Datagram Protocol, abrégé en UDP, est un protocole permettant l'envoi sans connexion de datagrammes dans des réseaux basés sur le protocole IP. Afin d'atteindre les services souhaités sur les hôtes de destination, le protocole utilise des ports qui constituent un élément essentiel de l'entête UDP. À l'instar de nombreux autres protocoles de réseau, l'UDP fait partie de la suite des protocoles Internet. Il intervient au niveau de la couche transport et joue ainsi le rôle d'intermédiaire entre la couche réseau et la couche application.

UDP est utile lorsque l'on n'a pas à vérifier chaque paquet. Ce protocole est beaucoup plus rapide que le protocole TCP dû au fait qu'il n'y a pas de vérifications à la réception.

Le meilleur exemple du protocole UDP est l'exemple de l'horloge. Un programme qui envoi l'heure à un ordinateur lorsque celui-ci le demande. Si jamais l'ordinateur ne reçois pas le paquet, ça n'a pas de sens de le renvoyer puis qu'entre temps, l'heure as changée.

La longueur du datagramme est définie dans le champ Longueur. Elle comprend la longueur de l'entête (8 octets) et la longueur des données utiles (en théorie maximum : 65 535 octets). En cas d'utilisation de IPv4, la limite effective pour les données utiles est de 65 507 octets, après déduction des entêtes IP et UDP. Dans IPv6, des paquets dépassant le maximum sont par ailleurs possibles.

La fin de l'entête UDP est constituée par la somme de contrôle qui sert à identifier les erreurs lors de la transmission. De cette façon, les manipulations des données transmises peuvent être identifiées, mais les paquets correspondants sont rejetés sans nouvelle demande. Pour calculer la somme, on utilise des parties

- De l'entête UDP

- Des données utiles

- Du pseudo entête (contient les informations de l'entête IP)

La somme de contrôle est facultative en IPv4, mais elle est toutefois utilisée par défaut par la plupart des applications. En l'absence de somme de contrôle, ce champ prend également la valeur 0. Si l'UDP est utilisé en association avec IPv6, la somme de contrôle est obligatoire.

Les différences avec le protocole TCP :

- UDP n'est pas un protocole orienté connexion

- Ce n'est pas un protocole sécurisé

- UDP envoie des paquets indépendants (datagrammes) depuis une source vers la destination

- Les paquets peuvent être perdus

- La vitesse est plus importante que la stabilité

- Son entête est de 8 octets

- UDP n'effectue pas de vérifications et donc ne peut être détecté dans le code

- UDP est utilisé pour les protocoles DNS, DHCP, SNMP, RIP, VoIP et TFTP

Avantages du protocole UDP :

- Il utilise des paquets de petite taille avec un petit en-tête (8 octets). Ce nombre réduit d'octets dans l'en-tête fait que le protocole UDP nécessite moins de temps pour traiter le paquet et moins de mémoire

- Il ne nécessite pas l'établissement et le maintien d'une connexion

- L'absence de champ d'accusé de réception dans l'UDP le rend plus rapide car il n'a pas besoin d'attendre l'ACK ou de conserver les données en mémoire

- Il utilise la somme de contrôle avec tous les paquets pour la détection des erreurs

- Il peut être utilisé dans les cas où un seul paquet de données doit être échangé entre les hôtes

Désavantages/inconvénients du protocole UDP :

- Il s'agit d'un protocole de transport sans connexion et peu fiable. Il n'y a pas de fenêtrage et aucune fonction permettant de s'assurer que les données sont reçues dans le même ordre que celui dans lequel elles ont été transmises

- Il n'utilise aucun contrôle d'erreur. Par conséquent, si UDP détecte une erreur dans le paquet reçu, il l'abandonne silencieusement

- Il n'y a pas de contrôle d'encombrement. Par conséquent, un grand nombre d'utilisateurs transmettant des lots de données via UDP peut provoquer un encombrement et personne ne peut rien y faire

- Il n'y a pas de contrôle de flux et pas d'accusé de réception des données reçues

- Seule la couche application s'occupe de la récupération des erreurs. Les applications peuvent donc simplement se tourner vers l'utilisateur pour lui envoyer à nouveau le message

- Les routeurs peuvent être négligents avec l'UDP. Ils ne retransmettent pas un datagramme UDP après une collision et rejettent souvent les paquets UDP avant les paquets TCP