Services des réseaux

Cours: UDP, services réseau et DHCP

Introduction :

Les réseaux informatiques utilisent des protocoles de transport pour permettre aux applications de communiquer

Les deux principaux protocoles sont :

UDP (User Datagram Protocol)

TCP (Transmission Control Protocol)

Dans cette section, nous étudions UDP et les raisons pour lesquelles on peut avoir besoin d'un protocole plus faible comme TCP

1/Le Protocole UDP

UDP est un protocole de transport non fiable, non connecté et rapide

Il n'effectue aucune vérification approfondie, ce qui le rend très léger

1.1 Structure d'un segment UDP

Un segment UDP contient deux parties :

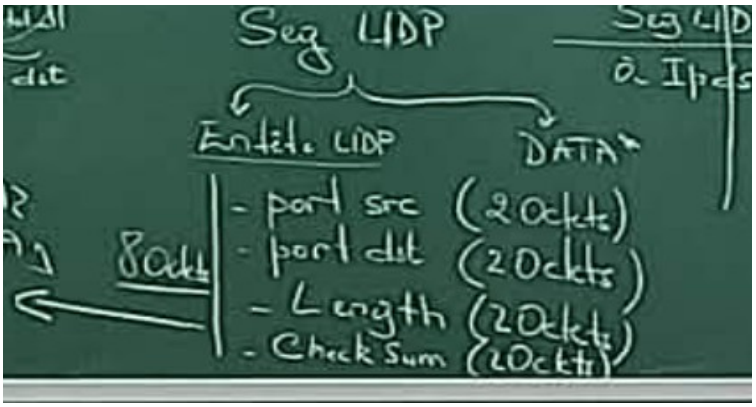
Partie1 : Les données DATA

Données envoyées par l'application

Partie2 : L'en-tête UDP(8octets)

L'en-tête est composé de 4 champs de 2 octets chacun :

Champ	Taille	Description
Port source	2 octets	Identifie le port de l'application émettrice
Port destination	2 octets	Identifie le port de l'application destinataire
Length	2 octets	Taille totale (en-tête +données)
Checksum	2 octets	Vérification simple d'erreurs



1.2 Limites de UDP

UDP présente deux problèmes principaux :

1)Fiabilité

2)séquencement

Lorsque deux chemins réseau de coût identique existent :

50% des paquets passent par le premier

50% par le second

- ➔ L'ordre d'arrivée peut être inversé

Par exemple :

La machine envoie deux segments, segment 1 puis segment 2 mais il y a plusieurs routes du même coût qui permettent d'émettre ces deux segments dans ce cas on a un ECMP ou il y a plusieurs routes vers le même réseau avec le même coût et le routeur envoie 50% dans la première route et 50% pour la 2éme route alors il peut être possible que le chemin dans la 2éme route et plus rapide ainsi le segment envoyé en deuxième sera le message reçu en premier lieu

UDP ne garantit pas l'ordre dans ce cas

Conclusion :

Pour les applications nécessitant fiabilité et ordre (ex : web, mail), UDP ne suffit pas

On utilise alors TCP

2/services réseau et applications

Un service réseau est une application qui fonctionne en permanence en arrière-plan.

On l'appelle un daemon ou un service

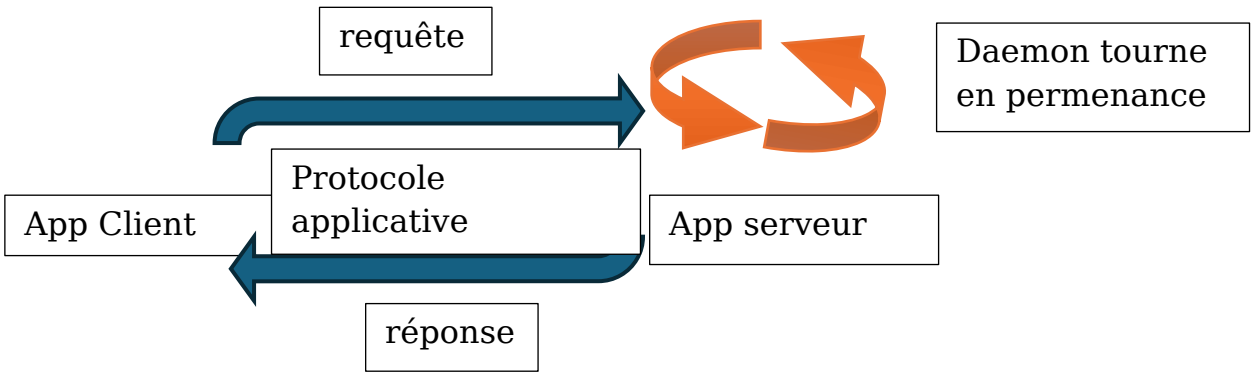
Exemples :

Serveur DHCP

Serveur DNS

Serveur Web

Serveur FTP



Lorsque le client et le serveur ne sont pas sur la même machine, ils doivent utiliser un protocole applicatif pour communiquer

3) Besoin de configuration réseau : rôle du DHCP

Pour fonctionner, la couche IP a besoin de :

1-adresse IP

2-masque de réseau

3-table de routage/ passerelle par défaut

4-DNS

Le protocole DHCP Dynamic host configuration Protocol permet d'attribuer automatiquement ces 4 informations a une appareille

4) Fonctionnement du DHCP :

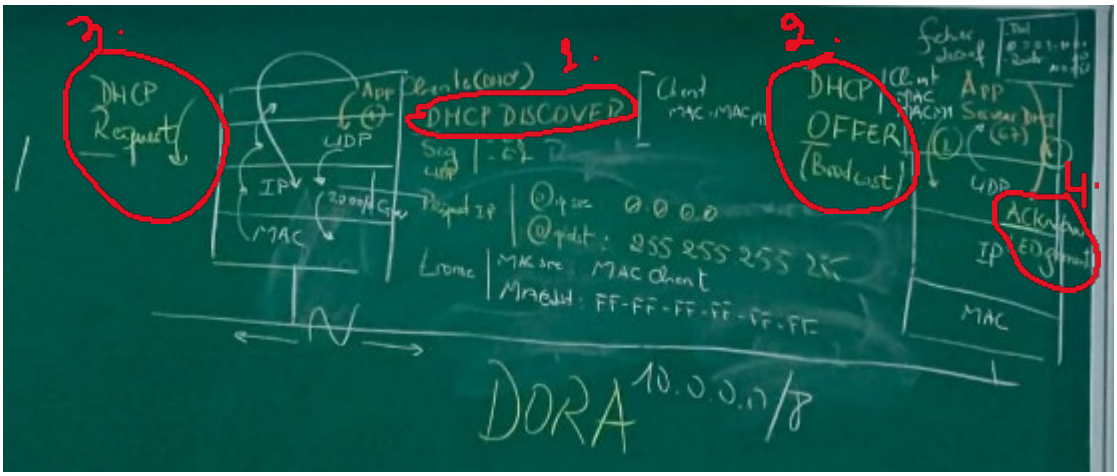
DHCP utilise un échange composé de 4 messages appelé DORA :

*Discover

*offer

*request

*acknowledge



4.1 DHCP Discover(client-> serveur)

Le client n’a pas encore d’adresse IP

Alors la couche application du client envoie un message DHCP DISCOVER aux serveurs

La couche UDP créer un segment contenant

Port source 68

Port destination 67

Remarque :

Le port client est toujours égale à 68

Le port serveur toujours égale à 67

La couche IP crée un paquet contenant

IP source (inconnue) : 0.0.0.0

IP destination 255.255.255.255(brodcast)

Remarque l’IP destination est brodcast ici car on ne sait pas l’adresse IP serveur

La couche MAC créer une trame contenante

Mac source : mac du client

Mac destination FF :FF :FF :FF :FF :FF (broadcast)

4.2 DHCP Offer(Serveur -> Client)

Le serveur reçoit la trame et vérifie :

Adresse MAC dans la couche mac

Adresse IP dans la couche IP

Port UDP =67 dans la couche UDP

Il répond avec UN DHCP OFFER suggérant une adresse IP dans sa fiche de règlement qui contient la plage d’adresses possibles à allouer

Puisque le client ne posséde pas encore d’adresse IP alors il ne sait pas son adresse IP d’où il vas répondre en brodcast aussi :

IP proposée

Masque

Default gateway

DNS

Server ID

Le problème ici c’est qu’au cours de la réponse au client supposant qu’on a 2 client du même port qui ont envoyé un DHCP DISCOVER c’est deux client ne peuvent pas être distingué que par la partie fixe du MSG DHCP qui contient le MAC CLIENT pour distinguer les clients ainsi on peut avoir la forme de message DHCP suivant :

Ou il y a 2 parties :

Partie fixe :

-client mac

-Your IP (c’est le champ qu’on veut modifier)

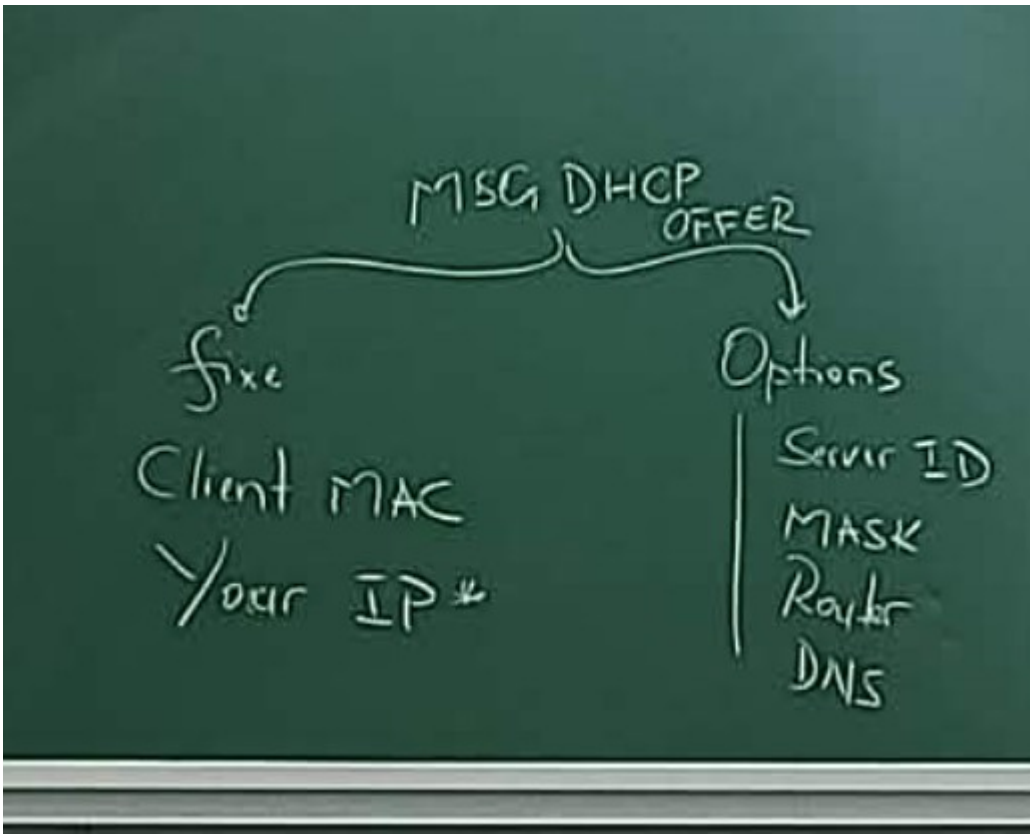
Partie options :

-server ID

-Mask

-Router

-DNS



4.3 DHCP Request (client -> serveurs)

Le client accepte une seule proposition DHCP

Il renvoie :

Un DHCP request mais en brodcast !

Pourquoi ?

Parce que même s'il a l'adresse IP destination du serveur il doit informer les autres serveurs qu'il ne vas pas utiliser leurs adresses IP pour qu'ils puissent l'allouer à d'autres machines

Ainsi le serveur rejeté il vas envoyer un DHCP reject pour libérer cette adresse IP

4.4 DHCP ACK :

Le serveur validé envoie un :

DHCP acknowledge, Le client peut désormais utiliser l'adresse IP attribuée

Si un serveur détecte un problème (IP déjà utilisée), il envoie :

DHCP Decline

5) Plusieurs serveurs DHCP dans le même réseau

Cela est possible mais à condition que chaque serveur possède un pool d'adresses différent sinon, conflit d'adresses garanti

6) renouvellement des adresses IP (brièvement) :

Quand un serveur DHCP te donne une adresse IP, il ne te le donna pas définitivement il te la prête pour une durée appelée Release Time qui vaut 8 heures :

Cela veut dire que l'adresse IP expire au bout de 8 heures si le client ne la renouvelle pas

Mais avant d'arriver à ces 8 heures, il y a deux étapes importantes :

- T1 renewal Time (4 heures)

  A la moitié du release time 8/2=4 le client envoie un DHCP Request en unicast au serveur DHCP qui lui a donné la première adresse

  Le but :

  Renouveler son bail avant qu'il n'expire

  Si le serveur répond avec un DHCP ACK, alors :

  -l'IP est modifié

  -le compteur repart à zéro -> il reste 8h d'utilisation de cette nouvelle adresse

- T2 Rebinding Time(3h)

  Si le serveur ne répond pas au moment T1 alors :

  Le client retente de renouveler son adresse cela veut dire il envoie des DHCP request à ce serveur pendant 3 heures

- T3 expiration(1h)

Pendant cette heure le serveur DHCP qui n’a pas répondue est déclaré comme défaillant et l’application DHCP lance une autre fois le processus DHCP cela veut dire elle va envoyer un DHCP DISCOVER pour trouver un autre serveur DHCP avant la fin de ses 8 heures et l’écrasement de son adresse IP