DHCP - DNS

Damien Gros

CEA

23 septembre 2023

Plan du cours

DNS

DHCP

Plan du cours

DNS

DHCP

Un peu d'histoire

Ce que l'on verra au prochain cours :

- Sur Internet (en dehors du LAN) les machines communiquent grâce à leur adresse IP : IPv4 ou IPv6.
- Ce sont les IP qui sont utilisées pour aller sur les sites Web ;
- Problèmes ?
  - Adresses IP difficiles à retenir pour des personnes lambda ;
  - Plusieurs sites sur la même adresse IP ;
  - Adresse IPv6 encore plus complexe.
  - Exemple : IPv4 de google.fr 173.194.34.24
  - Exemple : IPv6 de google.fr 2a00 :1450 :4007 :803 ::1018

Un peu d'histoire

- Donc on va utiliser des **noms** plutôt que des adresses IP.
- Un nom : www.google.fr, www.facebook.com, etc.
- Le nom www.google.fr : FQDN : `Fully Qualified Domain Name`
- Le principe : à partir d'un FQDN (abrégé par nom) on retrouve l'adresse IP (ou les adresses) qui lui est/sont associé.
- Principe appelé : résolution de noms mais aussi de resolver/solver de noms.

Aparté programmation C

- Il existe des fonctions en C capable de "résoudre les noms" :
- gethostbyname() et gethostbyaddr() ;

L'historique

- Au cours des années 1970, un fichier unique **hosts** (ou **hosts.txt**) contenait les noms de toutes les machines connectées à Internet avec leur IP correspondante ;
- Ce fichier était téléchargé/stocké sur le systèmes des postes clients.
- A chaque ajout de nouvelle machine, il fallait modifier ce fichier et le transmettre à tout le monde pour que les gens puissent accéder à votre machine (site web par exemple).
- On peut encore utiliser ce fichier aujourd'hui :
- Sur Linux /etc/hosts
- Sur Windows C :\Windows\System32\drivers\etc\hosts
- Syntaxe identique sur les 2 systèmes

Exemple de contenu du fichier hosts

```
127.0.0.1   localhost
173.194.34.24 google.fr
```

Création des DNS

- 1984 : Paul Mockapetris, mit au point un système de nommage hiérarchique distribué
- DNS : Domain Name System
- RFC 883 et 884, puis 1034 et 1035

Création des DNS

- Le DNS est une **base de données distribuée**
- Elle permet à des machines (bien précises) appelées **serveurs de nom** ou NS (name server) de contrôler des **zones** de cette base ;
- Cette base est accessible grâce à des mécanismes de type client-serveur.
- Un système de cache permet d'augmenter les performances de ces mécanismes tout en réduisant la charge des NS.

Domain Name System

Schéma 1

Résolution sans DNS

- On peut faire des résolutions de nom sans utiliser de DNS ;
- Il suffit de remplir les fichiers **hosts** (comme présenter précédemment).
- Le NIS (Network Information System), développé par Sun Microsystems appelé aussi YP (Yellow Page), crée un serveur sur le réseau LAN et peut résoudre certains noms (partage du fichier hosts)
- Le serveur WINS (Windows Internet Naming Service) des domaines Microsoft permet aussi la résolution de certains noms dits "netbios" (voir le fichier "lmhosts"). Cette résolution ne se fait que sur un LAN sauf mise en place de routage particulier.

La méthode DNS

- Les noms d'hôtes sont classés en une hiérarchie de domaines ;
- Un domaine est un ensemble de sites qui ont une relation entre eux.
- Exemple : **edu** aux USA regroupent les universités de ce pays.
- Dans les autres pays les sites sont regroupés sous un label constitué des deux lettres du code pays ISO-3166, fr France, de Allemagne etc...
- Puis on crée des sous-domaines pour définir un peu plus précisément l'organisation
- Exemple : toto.fr, www.toto.fr, learning.toto.fr
- Cette hiérarchie définit des domaines de niveau 1,2,3...

Distribution de nom par autorité

- Racine de l'arborescence **root** définie par un point : "."

Les serveurs root

- La racine **root** symbolisée par "." contient les références de tous les serveurs de domaines de niveau 0 (zéro) ;
- Elle est constituée par 13 serveurs répartis dans le monde qui, par un système de réplication, contiennent les mêmes informations

Les serveurs root

- Les serveurs root sont identifiés par les lettres de A à M et appartiennent tous au domaine ROOT-SERVERS.NET.
- Le serveur d'origine est géré par VeriSign Global Registry Services (A.ROOT-SERVERS.NET).
- Les autres serveurs sont des serveurs miroirs et sont administrés par :

Les serveurs root

- B.ROOT-SERVERS.NET : Information Sciences Institute USC (USA)
- C.ROOT-SERVERS.NET : PSINet
- D.ROOT-SERVERS.NET : University of Maryland (USA)
- E.ROOT-SERVERS.NET : NASA Ames Research Center (USA)
- F.ROOT-SERVERS.NET : Internet Software Consortium (USA)
- G.ROOT-SERVERS.NET : U.S. DOD Network Information Center (USA)
- H.ROOT-SERVERS.NET : U.S. Army Research Lab (USA)
- I.ROOT-SERVERS.NET : NordU (Suède)
- J.ROOT-SERVERS.NET : VeriSign Global Registry Services (USA)
- K.ROOT-SERVERS.NET : RIPE NCC (UK, Europe)
- L.ROOT-SERVERS.NET : ICANN (USA)
- M.ROOT-SERVERS.NET : WIDE Project (Japon).

La méthode DNS

- La racine de cette arborescence, de niveau 0, est un point.
- Il existe un groupe nommé **top level domain** (TLD), de niveau 1, composé de serveurs de plus haut niveau qui indiquent le mot juste sous la racine (com, fr, uk, edu.) .

Les Top-Level Domain

- Il existe deux types de domaines principaux **TLD** de premier niveau :
  - Les **ccTLD** (country-code TLD) : Domaines géographiques (ISO 3166) FR, CH, DE, US ;
  - Les **gTLD** (generic TLD) ;
    - Domaines génériques COM : Entreprises commerciales,
    - EDU : Établissements d'éducation,
    - GOV : Établissements gouvernementaux américains
- Adresses utiles : http ://www.iana.org/cctld/cctld.htm
  http ://www.iana.org/gtld/gtld.htm
- Jusqu'en 1998, la délégation de gestion d'un TLD était du ressort de l'IANA (Internet Assigned Numbers Authority).
- Actuellement c'est l'ICANN (Internet Corporation for Assigned Names and Numbers).

Domaines principaux

- Deux types de domaines principaux :
  - Domaines géographiques
    - Exemples : CH, FR, DE, US, TV (ISO 3166)
  - Domaines génériques
    - COM : Entreprises commerciales
    - EDU : Établissements d'éducation
    - GOV : Établissements gouvernementaux américains
    - MIL : Organisations militaires américaines
    - NET : Opérateurs de réseau
    - ORG : Organisations quelconques
    - INT : Organisations internationales

Top-Level Domain particuliers

- Parmi les **gTLD**, le domaine arpa(**Address and Routing Parameter Area**),est un TLD codé sur 4 lettres et dont l'utilisation est définie dans la RFC 3172.
- L'utilisation principale de ce domaine est la résolution inverse (adresse IP vers FQDN) .
- ATTENTION : La signification première de **ARPA** est **Advanced Research Project Agency**

Top-Level Domain particuliers

- Schéma : distribution des noms

Domaine et zone

- Pour être administré, un domaine peut-être découpé en zones, un serveur DNS différent s'occupant de chacune des zones.
- L'entreprise décide de faire une "délégation de la zone"
- Entreprise toto.fr délègue eleves.esiea.fr aux élèves de l'école.
- Le domaine « toto.fr » contient toutes les machines de TOTO.
- La zone « toto.fr » contient les machines « learning » « lalo » mais pas « bde » et « as ».
- La zone « eleves.toto.fr contient « bde » et « as ». « eleve.toto.fr » est aussi un domaine.

Domaine et zone

- Un domaine représente l'ensemble d'une sous-arborescence à partir d'un nœud donné.
- Une zone peut correspondre à un domaine, mais dans le cas général, elle englobe uniquement une partie du domaine, le reste étant délégué à d'autres serveurs de noms.
- La zone "fr" est restreinte au serveur de zone correspondant et contient la partie descriptive du domaine (incluant les informations sur les délégations de gestion du reste du domaine).
- Voir Schéma !

Interrogation serveurs de noms

- Pour une zone on définit généralement au moins deux serveurs de noms (pour la redondance, un maître et un esclave)
  - On dit que ces serveurs ont autorité sur la zone. On parle de serveurs « autoritatifs » ou « autoritaires »
  - L'un des serveurs est désigné comme maître et il y a périodiquement échange d'informations entre le serveur maître et le(s) serveur(s) esclave(s) pour une synchronisation.
  - Un serveur peut gérer plusieurs zones de domaines qui peuvent être différents. Exemple : toto.fr et toto.eu
- Pour obtenir le numéro IP de toto.fr, un hôte réalisera les opérations suivantes (si /etc/hosts, Wins et NIS non utilisés) :
  - Envoyer sa requête à un serveur DNS
  - Si celui-ci ne connaît pas la réponse, il contacte un serveur DNS racine.
  - Puis on redescend dans la hiérarchie jusqu'à obtenir l'information désirée.

Interrogation serveurs de noms

- Schéma !

Interrogation serveurs de noms

- Il existe deux modes d'interrogation des serveurs.
- Modes itératif, récursif
  - En mode récursif, le serveur interrogé prend en charge les appels (récursifs ou itératifs) à d'autres serveurs nécessaires pour résoudre la recherche.
  - En mode itératif, il fournit l'information la plus détaillée dont il dispose, le programme client prenant en charge l'appel à d'autres serveurs. Un serveur de noms peut refuser d'honorer les requêtes récursives. C'est le cas des serveurs de premier niveau très sollicités.
- Utilisation de caches (noms de machines récemment utilisés et numéros IP correspondant) : lorsqu'un client demande un nom, le serveur vérifie au préalable que celui-ci n'est pas dans la mémoire cache.

Interrogation serveurs de noms

- Schéma serveur itératif/récursif
- Schéma serveur autoritaire

Ressource Record

- La base de données DNS ne gère pas que des adresses IP mais aussi des informations sur les serveurs de noms.
- Sur UNIX on trouve ces informations dans un fichier généralement nommé named.hosts.
- Chaque ligne de ce fichier est appelé RR «Ressource Record».
- A chaque RR est associé un type
  - Ex : adresse IP est un RR de classe A (attention à la confusion avec les classes d'adresse IP) AAAA pour une adresse IPv6.
  - CNAME indique un alias vers le nom canonique.
  - MX (Mail Exchange), spécifie un serveur de mails (son adresse IP).

Ressource Record

- Les enregistrements NS associés à un enregistrement A permettent de définir une délégation de zone.
- Ils sont appelés **Glue Record**.
- Ce sont eux qui construisent l'arborescence DNS.

```
eleves.toto.fr. IN NS nseleves.esiea.fr.
nseleves.toto.fr. IN A 149.62.158.51
```

Ressource Record

- Base de données pour les requêtes inverses (Reverse Mapping).
- Il existe un domaine principal in-addr.arpa.
- Ce domaine contient l'adresse des machines en notation inversée.
- Exemple 149.62.158.51 devient 51.158.62.149.in-addr.arpa .

Ressource Record

- Base de données pour les requêtes inverses
- Exemple de fichier named.rev le domaine 158.62.149.in-addr.arpa

```
@IN SOA serveur.toto.fr.
admin.toto.fr. (
960925 ;numéro de série
360000 ; mise à jour
3600 ;tentative après échec
3600000 ;délai d'expiration
3600 ; ttl par défaut )
IN PTR serveur.toto.fr
```

Ressource Record

```
damien@ossus :3A/cours_reseau_2014_2015/cours_5% dig MX google.fr

; <<>> DiG 9.9.4-RedHat-9.9.4-14.el7 <<>> MX google.fr
;; global options : +cmd
;; Got answer :
;; ->>HEADER<<- opcode : QUERY, status : NOERROR, id : 27543
;; flags : qr rd ra; QUERY : 1, ANSWER : 5, AUTHORITY : 0, ADDITIONAL : 2

;; OPT PSEUDOSECTION :
; EDNS : version : 0, flags :; udp : 4000
;; QUESTION SECTION :
;google.fr IN MX

;; ANSWER SECTION :
google.fr.google 511 IN MX 30 alt2.aspmx.l.google.com.
google.fr.google 511 IN MX 40 alt3.aspmx.l.google.com.
google.fr.google 511 IN MX 50 alt4.aspmx.l.google.com.
google.fr.google 511 IN MX 10 aspmx.l.google.com.
google.fr.google 511 IN MX 20 alt1.aspmx.l.google.com.
```

Serveur DNS

- /etc/resolv.conf : sous Linux (nameserver)
- Propriété de la carte sous Windows

La sécurité dans DNS

- DNSSEC ;
  - Assurer que la réponse est bien celle attendue (DNS menteur)
  - Les enregitrements sont signés par le serveur faisant autorité sur la zone
  - Possibilité de vérifier ces signatures (manuel ou automatique)
- DNS over TLS,
- DNS over HTTP(s) ;
  - Assurer la confidentialité de l'échange
  - N'assure pas l'intégrité de la réponse
  - Contournement des restrictions mises en place par les opérateurs/autres

Plan du cours

DNS

DHCP

Accès à Internet

- Pour accéder à Internet, un hôte doit nécessairement avoir au minimum 3 informations sous forme d'adresses IP :
  - Une adresse IP, pour lui même afin que les autres nœuds réseau puisse lui répondre.
  - L'adresse IP de la passerelle du réseau local sur lequel il se trouve qui va lui permettre de communiquer au delà de son LAN.
  - L'adresse IP d'au moins un serveur de noms DNS, afin qu'il puisse résoudre les noms FQDN et trouver l'adresse IP correspondante

Accès à Internet

- Pour disposer de ces 3 informations, il existe deux méthodes.
  - L'une des méthodes est manuelle et on doit disposer des droits administrateurs nécessaires pour l'effectuer.
  - L'autre est automatique en utilisant le réseau local lorsque la machine démarre. Pour cela il faut que le réseau local dispose d'un serveur adéquate. Ce type de serveur est appelé serveur **DHCP** (`Dynamic Host Configuration Protocol`).

Accès à Internet

- Sous Linux :
  - ifconfig eth0 IP.IP.IP.IP
  - route (on verra cette commande au prochain cours)
  - /etc/resolv.conf

Réglages Manuelles

- Avantage :
  - Pas de nécessité de la présence d'un serveur DHCP sur le LAN
- Inconvénients :
  - Il faut connaître les données du réseau sur lequel on branche la machine (Adresse passerelle, Adresse DNS, adresse du réseau)
  - Si on déplace la machine sur un autre réseau, il faut recommencer les réglages.

Réglage automatique par serveur DHCP

- DHCP est défini dans les RFC 1531, 2132, etc.
- DHCP caractéristiques :
  - DHCP est une extension du protocole BOOTP qui permet à un client sans disque dur (terminal X, imprimante, etc.) de démarrer et de configurer automatiquement IP.
  - Les informations échangées sont plus complètes que sous BOOTP
  - Non limité aux réseaux locaux (« routable » sous certaines conditions (relais DHCP))
  - Totalement automatique pour la machine cliente

DHCP la pile de protocoles

- Utilise UDP (UDP sera détaillé au prochain cours)
- Passe les routeurs
- utilise les ports 67 (serveur) et 68 (client)
- Plusieurs serveurs
  - Redondance
  - Chaque serveur « offre » une configuration
  - Le client choisit celle qui lui convient

Echange DHCP

schéma 1 DHCP

Le client au démarrage

- Initialement, le client :
  - Il n'a d'adresse IP
  - Pas de serveur DHCP connu
  - Possède seulement une adresse MAC
  - Requête de broadcast sur le réseau au niveau 2
  - Broadcast Ethernet (FF-FF-FF-FF-FF-FF)
  - Et Broadcast IP (255.255.255.255)

Découverte des serveurs DHCP par le client

- Broadcast datagramme UDP
  - Port client 68 vers serveur port 67
  - Message = « DhcpDiscover »
- Routeurs spéciaux
  - DHCP/BOOTP relay
  - Ne font que transférer les messages DHCP

Réponse du serveur

- Le client est-il connu ?
  - Si l'adresse MAC est connue délivrance d'une adresse IP fixe possible.
  - Cette politique est gérée par l'administrateur
- Choix d'une adresse IP dynamique ou fixe.
- Validation de l'adresse IP par un ping, si pas de réponse alors l'adresse est validée par le serveur
- Envoi de l'offre : « DHCPOFFER »

Le choix de l'adresse IP par le serveur

- Le client a déjà une IP alors attribution de la même
- Le client a déjà eu une adresse IP encore disponible, alors attribution de la même.
- Le client demande une IP particulière disponible, alors, attribution de l'adresse demandée.
- Prendre une adresse IP libre quelconque dans un spool d'adresses.

Envoi de la réponse

- Selon IP Client :
  - Déjà disponible : Envoi unicast (IP) de la réponse
  - Pas encore disponible : Envoi broadcast (IP) de la réponse
- Selon position sur le réseau
  - Même réseau : Envoi unicast (Ethernet) la réponse au client
  - DhcpDiscover a été routé Envoi unicast (Ethernet) la réponse au relais

Choix d'une adresse par le client

- Le client reçoit plusieurs offres
- Choix d'une offre selon options du client
- Envoi d'un message « DhcpRequest »
  - Broadcast avec ID du serveur choisi
  - Tous les serveurs reçoivent le choix du client : Offre non choisi alors annule l'offre pour le serveur
  - Si choisi alors l'offre est validée

Validation finale de l'adresse IP

- L'IP a été attribuée avant la validation du client.
  - Oui alors envoi message « DhcpNack » par le serveur.
  - Non alors envoi message « DhcpAck » par le serveur. Son message contient éventuellement d'autres informations (serveur DNS, Passerelle, etc.)
- Envoi par broadcast IP
  - Le client reçoit l'offre finale
  - Les serveurs retirent l'adresse de leur stock
- Le client teste l'adresse allouée
  - Si une erreur : envoi message « DHCPDECLINE », Attend 10 secondes, Recommence la découverte des serveurs

Notion de bail

- Une adresse obtenue par DHCP est valide
  - Eternellement
  - Pour une période donnée (bail, lease)
    - Le bail est la durée pendant laquelle l'IP ne sera pas offerte de nouveau
    - Un bail peut être prolongé
  - Une adresse peut être rendue
    - Message « DHCPRELEASE »
    - Unicast au serveur bailleur