SNT 2.1 ADRESSES SYMBOLIQUES ET SERVEURS DNS

Oral : à votre avis, comment les ordinateurs sont reliés entre eux ? Comment identifier un ordinateur ?

Repères historiques :

- Vidéo Delagrave (≈ 3 min)

- Grâce à sa souplesse et à son universalité, internet est devenu le moyen de communication principal entre les hommes et avec les machines.

Vidéo : une brève histoire de l'internet (env. 5min) → attention, petite erreur à 1:16, le réseau Arpanet n'utilisait pas vraiment l'échange de paquets, c'est Cyclades – comme on le verra plus tard – qui introduira cela.

- Pages 14/15 : passer rapidement sur Arpanet et Cyclades, on y reviendra plus tard

- Internet a fait progressivement disparaître beaucoup des moyens de communication précédents : télégramme, télex, le courrier postal pour une bonne partie, et bientôt le téléphone fixe grâce à VoIP (voix sur IP). Son trafic prévu pour 2021 est de 3 300 milliards de milliards d'octets ($3{,}3 \times 10^{21}$ octets).

Page 16 : doc.1 Nom de domaine
doc.2 Adresse IP
Page 22 : doc.2 La transition vers l'IPv6

A dire : les premiers chiffres d'une adresse IP ne permettent pas vraiment de trouver la location… En effet, des groupes sont réservés pour certains AS (systèmes autonomes), donc pour certains pays, mais ils peuvent être variés et changer. Par exemple, le 19/07/2019, on trouvait ces groupes pour le Paraguay :

```
# Report generated on Fri Jul 19 10:14:30 2019
# by http://software77.net/geo-ip/
# Registry : LACNIC
# Records found : 101 BEFORE flattening (As they appear in the database)
# Records : 92 AFTER flattening (Adjoining CIDR blocks concatenated into single blocks where possible)
```

45.160.32.0/22	45.228.60.0/22	138.186.60.0/22	181.120.0.0/13	200.3.248.0/21
45.161.236.0/22	45.228.136.0/22	138.219.8.0/22	181.174.160.0/22	200.7.14.0/24
45.162.180.0/22	45.229.168.0/22	143.202.208.0/22	186.0.188.0/22	200.9.4.0/22
45.163.188.0/22	45.234.84.0/23	143.255.140.0/22	186.2.192.0/19	200.10.141.0/24
45.165.52.0/23	45.234.86.0/24	160.238.184.0/22	186.2.224.0/20	200.10.228.0/22
45.169.112.0/22	45.235.120.0/22	164.163.184.0/22	186.16.0.0/15	200.12.146.0/24
45.170.104.0/22	45.236.244.0/22	167.250.36.0/22	190.2.192.0/20	200.26.176.0/21
45.170.128.0/22	45.237.44.0/22	168.90.176.0/22	190.23.0.0/16	200.61.224.0/20
45.172.228.0/22	45.238.36.0/22	168.194.240.0/22	190.52.128.0/18	200.85.32.0/19
45.173.180.0/24	45.239.44.0/22	168.195.224.0/22	190.93.176.0/22	200.108.128.0/20
45.175.156.0/22	131.72.24.0/22	170.82.144.0/22	190.104.128.0/18	200.115.16.0/23
45.176.86.0/23	131.100.184.0/22	170.83.240.0/22	190.112.208.0/21	200.124.120.0/24
45.177.16.0/22	131.108.192.0/22	170.84.172.0/22	190.113.92.0/22	201.131.51.0/24
45.177.204.0/22	131.161.252.0/22	170.233.216.0/22	190.114.224.0/21	201.217.0.0/18
45.178.48.0/22	131.196.192.0/22	170.238.16.0/22	190.121.160.0/20	201.220.25.0/24
45.179.152.0/22	132.255.164.0/22	170.254.216.0/22	190.128.128.0/17	201.222.48.0/21
45.179.192.0/22	138.59.164.0/22	177.250.0.0/15	190.211.240.0/22	
45.180.180.0/22	138.99.100.0/22	179.0.26.0/24	191.97.120.0/21	
45.226.180.0/22	138.122.160.0/22	181.40.0.0/16	200.1.200.0/21	

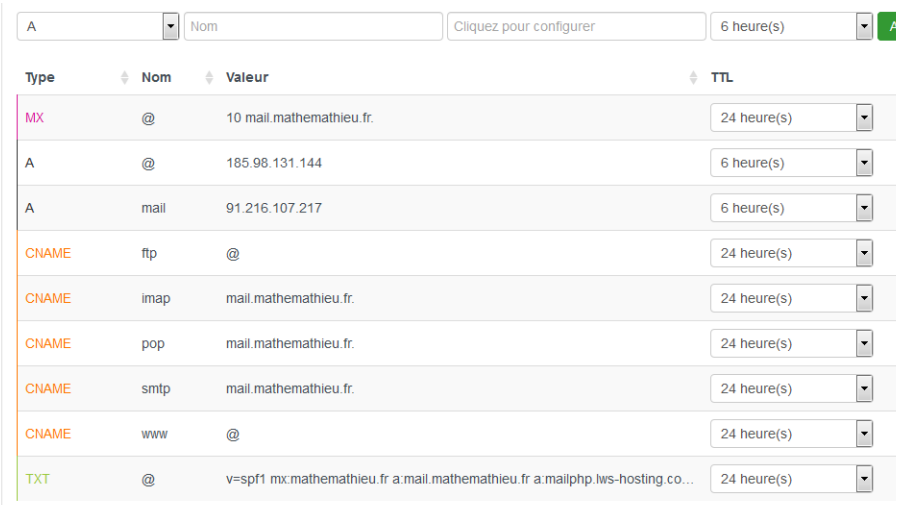
Vidéo (env. 4 min 30 s) : comprendre le DNS en 5 minutes

Page 17 : doc.3 Le système DNS

A savoir : en 2015, les Etats-Unis, sous pression internationale (de l'UE, de nombreux pays d'Asie et d'Amérique du Sud), ont renoncé à des décennies de gérance du DNS racine via l'organisme ICANN qui était rattaché au *Département du Commerce* de l'administration américaine et est désormais placé entre les mains d'une organisation internationale.

Remarque : on entend souvent parler de « la » racine (ou *server root*), mais il y en a plusieurs.

Le résolveur DNS garde en mémoire les résultats ; si on cherche deux fois le même nom de domaine, le résolveur de mon FAI répondra très vite la seconde fois, car il a déjà en mémoire le résultat. La durée de cette mémoire dépend du TTL (*Time To Live*), qui peut être différent pour chaque nom de domaine. Cela se configure →
Mais il vaut mieux éviter de mettre un TTL trop bas pour ne pas finir sur une liste de spam.



Sans compter que s'il y a une panne (ou un DDoS = *Distributed Denial of Service*, voir plus bas), toute l'infrastructure est HS après TTL minutes, tandis que s'il y a un cache plus long, une partie des utilisateurs ne sera pas impactée.

Le résolveur DNS ne consulte pas une racine à chaque fois, il demande la liste des serveurs qui gèrent les TLD, et la garde en cache pendant 2 jours. La liste des serveurs racines est gardée en cache pendant 6 jours.
Voilà pourquoi, lorsqu'on change d'hébergeur (du nom de domaine), cela peut mettre jusqu'à 2 jours, le temps que les caches soient actualisés.

Contrairement à la croyance populaire, il n'y a plus de nos jours physiquement et uniquement 13 serveurs racine du DNS, mais plutôt 13 « identités de serveur » (A, B, C, … , M) ayant chacune une adresse IP.
Les « serveurs racines » sont donc un réseau de milliers de serveurs dans de nombreux pays à travers le monde : 997 sites dans 53 pays en juillet 2019 (il y avait 130 sites en 2007…). Montrer la map et zoomer dessus : https://root-servers.org/
Douze organisations contrôlent ces serveurs, deux sont européennes, une japonaise, les autres étant américaines. Neuf de ces serveurs ne sont pas de simples machines mais correspondent à plusieurs installations réparties dans des lieux géographiques divers. La racine « I », par exemple, est située dans 25 pays différents. Voir une carte.
Chaque serveur racine est une copie et aucun d'entre eux n'est plus spécial que les autres. Le véritable serveur maître à partir duquel les copies sont effectuées n'est pas l'un des serveurs racine publics.
Si l'un ou quelques-uns des *root servers* ne répondent plus, la charge est répartie entre les serveurs qui subsistent. Si aucun d'entre eux ne pouvait répondre aux requêtes, les noms de domaines deviendraient progressivement inaccessibles, au fur et à mesure que les informations dans les caches parviendraient à expiration, c'est-à-dire environ 2 % par heure d'indisponibilité totale.
L'adresse de la plupart des serveurs n'est pas publiée pour éviter les attaques ciblées.
Il n'est pas rare que l'un des serveurs fasse l'objet d'une attaque par déni de service, sans que cela affecte de façon perceptible la qualité du fonctionnement du DNS dans son ensemble.

Certaines attaques de grande ampleur ont cependant eu lieu au XXI^{e} siècle :
- Le 21 octobre 2002, la racine complète du DNS a fait l'objet d'une attaque de grande ampleur pendant une heure, les treize serveurs A à M étant visés. Pendant cette attaque, 7 serveurs sur 13 ont vu leurs performances dégradées en raison d'un flux de 100 000 à 200 000 requêtes par seconde vers chacun des serveurs. Toutefois, l'attaque n'a pas provoqué de grandes perturbations du réseau mondial, ce qui montre la robustesse du système. Selon le président-directeur général de Verisign, qui gère deux serveurs racine, l'ensemble des requêtes aurait pu être assuré par un seul serveur.

L'attaque a été réalisée selon la méthode DDoS (déni de service). Les pirates ont pu, grâce à un parc de machines très important, générer un nombre de requêtes deux à trois fois supérieur à la capacité de charge des treize serveurs visés, soit quarante fois le volume habituel des requêtes.
Le système *anycast* a été mis en place après cette attaque pour neutraliser les attaques de type DDoS.
- Le 6 février 2007, les serveurs F, G, L et M ont été attaqués pendant 24 heures. Les serveurs G et L ont été affectés sérieusement, tandis que F et M ont rapporté une charge inhabituelle. L'impact sur M a été amoindri grâce à *anycast*.
La source s'avère être un réseau *botnet* de 5 000 machines essentiellement basées en Corée du Sud et dirigé depuis les États-Unis.
- Le 30 novembre 2015 (de 06:50 UTC jusqu'à environ 09:30 UTC) et le 1er décembre 2015 (de 05:10 UTC à 06:10 UTC), les 13 serveurs racines ont fait l'objet de deux attaques DDoS, causant des délais d'attente sur les serveurs racine B, C, G et H. Environ 5 millions de requêtes ont été envoyées par seconde vers les serveurs avec deux domaines uniques à l'origine de l'attaque, un pour chaque attaque. Trois des treize serveurs racine ont subi des ralentissements, mais l'impact sur l'ensemble d'internet est resté limité.
- Le 21 octobre 2016, DDoS de plus d'un téraoctet par seconde visant le service Dyn Managed DNS. De nombreux sites qui utilisent ce service, tels que Twitter, Ebay, Netflix, GitHub, PayPal, sont inaccessibles pendant une dizaine d'heures. Les attaquants se sont servis d'objets connectés piratés (comme des caméras de surveillance) infectés par le logiciel malveillant nommé *Mirai* pour relayer le flux de paquets massif.

Sur les *root servers* : voir TP4 (TP - Internet(Web)4 pharming et contrôle d'Internet)

Vidéo (env. 16 min) : DNS – la surveillance de masse facile

Exemples : à l'aide du site my-ip-finder.fr ou d'un autre (mots clés : whois, dnslookup, ip location)…
1) Trouver l'adresse IP du domaine www.pixees.fr *(réponse : 128.93.162.128)*
2) Trouver le nom de domaine associé à l'adresse IP 188.165.55.58 *(réponse : reopen.info)*
Dans quelle ville est localisé le serveur sur lequel est le site ? *(réponse : Roubaix ?)*
Quel est le fournisseur du serveur ? *(réponse : kimsufi ou OVH)*

Remarque : avec un whois, les sites nous donnent la location… Sauf qu'elle diffère selon les sites, c'est imprécis, attention ! Par exemple pour mon site www.mathemathieu.fr, géré par LWS, ça renvoie parfois Ile-de-France, parfois Poitou-Charentes…

Présentation des commandes (pour Windows) **ipconfig**, **ping** et **traceroute/tracert** sur un exemple, si besoin avec le logiciel Filius, qui sera utilisé au prochain TP.
Présentation également du site geotraceroute.com qui permet de visualiser sur une carte le trajet effectué entre une source choisie (prendre Toulouse) et une adresse IP ou un site.

À lire :

Comment les autorités peuvent bloquer un site Internet ?

Tout ce que vous devez savoir sur le piratage DNS

Piratage : internet subit une attaque d'ampleur

Une attaque par déni de service, qu'est-ce que c'est ? (vidéo, ≈ 3 min)