ACTIVITE 2 – FAUT-IL CONNAITRE SON ADRESSE IP ?

Comprendre la forme des adresses IP

2.1

Observer ces deux brefs extraits d'un tableau de plages d'adresses IP allouées à différents opérateurs en France :

IP début	IP fin	Nbre	Date	Propriétaire
2.0.0.0	2.15.255.255	1048576	12/07/2010	Orange S.A.
5.39.0.0	5.39.127.255	32768	15/05/2012	OVH SAS
5.42.160.0	5.42.191.255	8192	18/05/2012	Blizzard Entertainment
5.48.0.0	5.51.255.255	262144	22/05/2012	Bouygues Telecom SA
5.57.96.0	5.57.127.255	8192	01/06/2012	Société Réunionnaise de Radiotéléphone SCS
5.135.0.0	5.135.255.255	65536	06/07/2012	OVH SAS
…	…	…	…	…
212.194.0.0	212.195.255.255	131072	30/08/2000	Bouygues Telecom SA
212.197.192.0	212.197.255.255	16384	25/08/2000	Atos Euronext Market Solutions SAS
212.198.0.0	212.198.255.255	65536	19/03/1998	NC Numericable S.A.
212.208.0.0	212.208.127.255	32768	06/02/1998	Verizon France SAS

Qu'en déduisez-vous sur la forme des adresses IP en général ? Et saurez-vous expliquez pourquoi elle a cette forme ?

Une adresse IP se note en 4 nombres allant de 0 à 255, séparés d'un point. Pour chaque nombre, il y a donc 256 possibilités, ce qui correspond à 2^8. Il faut bien sûr avoir en tête que tout, en informatique, est enregistré sous forme binaire. Un nombre de 0 à 256 est codé sur 8 chiffres binairs, on dira « 8 bits ». Or 8 bits, pour des raisons historiques liées à certains composants des premiers ordinateurs électroniques et au fait qu'il s'agit d'une puissance de 2 proche de notre base 10, est devenue la norme de l'unité de mesure d'un volume d'information. 8 bits, c'est 1 octet (*byte* en anglais, à ne pas confondre avec *bit*), noté «o», comme dans Mo ou Go.
Une adresse IP est donc codée sur 4 octets, présentés en notation décimale et séparés par un point pour faciliter la lecture humaine. Sinon, toujours en décimal, 5.39.0.0 devrait s'écrire 86 441 984 (soit $5x2^{24} + 39x2^{16}$). Cela ne semble pas forcément plus compliqué, mais le lien avec la valeur binaire équivalente n'apparaît plus, ce qui est problématique, on le verra, pour identifier la partie « réseau » de cette adresse.
On remarque par la même occasion que le nombre d'adresses disponibles sur une page donnée d'adresses IP est une puissance de 2, et que ces plages sont de proportion très variables.

2.2

Les ordinateurs manipulent des nombres binaires (composés seulement de 0 et de 1). Convertissez les adresses suivantes, soit de la notation décimale vers la notation binaire, soit l'inverse. Si vous ne savez pas comment faire, demandez à votre professeur de vous donner une méthode.

IP en décimal (base 10)	IP en binaire (base 2)
91.198.174.192	01011011.11000110.10101110.11000000
144.76.131.212	10010000.1001100.10000011.11010100

2.3

Les deux adresses précédentes correspondent à des serveurs de sites web, lesquels ? Pour le savoir, utilisez la commande « ping -a » suivie de l'adresse IP (dans l'Invite de commande de Windows – demandez à votre professeur comment l'ouvrir), ou bien allez sur un site comme https://ping.eu/ , en utilisant le service « Reverse lookup ».

text-lb.esams.wikimedia.org
edna.framasoft.org
Ici on peut faire une première mention du principe du DNS, mais on l'examinera de plus près ensuite

2.4

Etant donnée la nature des adresses IP et chaque adresse correspondant théoriquement à une machine, calculez combien de machines peuvent théoriquement être connectées à Internet. Qu'en pensez-vous ? Est-ce suffisant ?
D'après vous, comment pourrait-on s'y prendre pour augmenter la capacité du réseau ?

2^{32} = 4 294 967 296

C'est moins que le nombre d'humains susceptibles de se connecter aujourd'hui, mais surtout c'est un chiffre déjà dépassé compte tenu de la multitudes d'appareils que certains utilisent dans leur vie professionnelle comme personnelle. Ainsi, en 2016, on dénombrait 16 milliards d'objets connectés (tout type confondu), dont 1,6 milliards d'ordinateurs et 7 milliards de mobiles.

Les élèves pourront proposer qu'on allonge l'adresse comme on l'a fait pour les numéros de téléphones dans les années 90 (ce qui correspond en substance à la solution robuste d'IPv6), ou bien d'espérer que tout le monde ne se connecte pas en même temps et de distribuer à la demande les adresses, ou bien de partager une même adresse à plusieurs (mais comment ?)

Le problème de la saturation des adresses IP préoccupe depuis les années 1990. Une solution majeure a été mise en place il y a plus de 20 ans mais n'est pas encore vraiment appliquée : elle a consisté à élargir considérablement le nombre de bits sur lesquels est codée l'adresse, passant de 32 bits à 128 bits. On parle d'**IPv4** pour désigner les adresses telles qu'on les a écrites jusqu'ici, **IPv6** pour la nouvelle version, qui donne par exemple ceci :

`2001:0db8:0000:85a3:0000:0000:ac1f:8001`

soit 8 nombres de 4 chiffres écrits en notation hexadécimale (base 16). Avec 2^{128} possibilités, c'est-à-dire environ $3{,}4 \times 10^{38}$, il y a de quoi voir venir (on pourrait à peu près donner une adresse à chaque atome composant le corps de chaque humain – cherchez d'autres ordres de grandeur pour réaliser à quel point c'est énorme).

Dans la pratique, on se contente pour le moment de l'IPv4, grâce à des principes qu'on va découvrir dans l'exercice suivant.

Les adresses IP de mes objets connectés sont-elles des données personnelles et sensibles, au même titre que mon n° de téléphone ?

Puisqu'il est nécessaire que chaque machine connectée à Internet ait une adresse IP pour communiquer sur le réseau, alors votre smartphone ou votre ordinateur, lorsqu'ils sont connectés, en ont une. Intéressons-nous au cas du smartphone qui, par principe, est itinérant, c'est-à-dire se connecte régulièrement en différents points du réseau. D'après-vous, a-t-il une adresse IP unique et fixe ? Et faut-il connaître son adresse IP comme il est bon de connaître son numéro de téléphone ? Est-ce une donnée personnelle qu'il faut protéger, ne pas divulguer à n'importe qui ?

2.5

Dans un navigateur, testez cette adresse : http://217.41.39.137:81/
Qu'en pensez-vous et comment cela nous conduit-il à répondre aux questions qu'on vient de soulever sur le caractère personnel de votre adresse IP ?

C'est une webcam, ce qui peut sembler assez inquiétant en matière de **sécurité** ! N'importe qui peut-il me regarder à travers la caméra de mon smartphone ou la webcam de mon ordinateur ?
Remarquez que l'adresse IP, il y a un numéro de port. C'est par ce type de code qu'on accède à différents services d'une machine, s'ils ne sont pas fermés ou protégés par un **firewall** (expliquer ici son rôle)

2.6

Cherchez l'adresse IP de votre smartphone ou de celui d'un camarade qui peut se connecter à Internet (dans les paramètres, sous Android, aller dans « A propos du téléphone » puis « Etat »). Notez là :
Allez sur https://www.mon-ip.com/ ou, dans le moteur de recherche d'un smartphone, tapez « mon adresse IP publique » et suivez l'un des premiers liens. Notez l'adresse indiquée.

Normalement, on devrait constater que l'adresse indiquée dans les paramètres du téléphone n'est pas la même que l'adresse publique, c'est en fait une adresse interne au réseau de notre opérateur téléphonique.

Coupez la connexion Internet du smartphone (passez en « mode avion » par exemple) puis reconnectez le. Rafraichissez l'affichage de la page qui indique votre adresse publique. A-t-elle changé ? Notez la nouvelle adresse.

En effet, normalement, elle change.

Dans un navigateur, allez sur le site https://ipgetinfo.com et cherchez des renseignements sur les adresses IP que vous avez relevées. Que remarquez-vous ?

Si la géolocalisation est possible (pas toujours, et pas toujours fiable), on peut parfois constater que les serveurs du FAI auxquels on s'est successivement connecté et qui font office de passerelle vers l'Internet se situent dans différentes régions en France.

Si vous pouvez vous connecter à une borne wifi, observez la manière dont cela change à la fois l'adresse publique du smartphone et l'adresse visible dans les paramètres (à défaut, sachez que cette dernière serait probablement du type 192.168.0.x si vous vous connectiez à une box comme vous pouvez en avoir une chez vous). Comment expliquez-vous ces changements d'adresses et cette différence entre l'adresse publique et l'adresse visible dans les paramètres du smartphone ?

Ici il s'agit de faire comprendre la différence entre l'adresse privée, allouée au sein d'un réseau local (par exemple le réseau du lycée, ou celui de la maison, via la box), et l'adresse publique, qui est la même pour toutes les machines connectées au même réseau local, car il s'agit de l'adresse de la passerelle qui fait le lien entre ce réseau local et Internet. En plus d'apporter une réponse à pratique à la difficulté de la saturation des adresses IPv4, c'est une bonne manière revenir sur l'idée fondamentale qu'Internet est un réseau de réseaux, l'interconnexion de tous les réseaux qui veulent bien s'interconnecter (et non pas de tous, car certains restent entièrement privés).
Ici, il faut expliquer le rôle de la passerelle (qui détecte quand l'adresse de destination d'un message envoyé par l'une des machines du réseau ne correspond pas à une adresse locale, et ainsi l'achemine vers Internet), qui en général ont une fonction de NAT (Network Adress Translation : elles opèrent la « translation » entre les deux types d'adresses, privée et publique). On peut éventuellement introduire le DHCP, qui assure une allocation dynamique, à chaque connexion, des adresses IP disponibles sur un réseau. C'est en général un service actif sur une box, et c'est un service équivalent qui explique qu'à chaque connexion au réseau 4G, le smartphone reçoive une adresse IP différente sur le réseau de l'opérateur).
On peut enfin évoquer les plages réservées pour les adresses privées.

2.7

D'après ce que votre professeur a expliqué, est-il possible :

- Qu'une personne malveillante, qui n'est pas en contact avec vous mais qui a décidé de retrouver votre adresse IP la retrouve et se connecte à votre smartphone ou ordinateur personnel ?

Théoriquement ce n'est pas possible, en tout cas pour les smartphones, qui ont toujours une adresse allouée dynamiquement, ie qui change tout le temps. L'IP de son smartphone n'est donc pas une donnée personnelle au même titre que le numéro de téléphone ou l'adresse e-mail, par exemple. Elle n'est personnelle que de manière très éphémère et ponctuelle.

- Qu'une enquête policière détermine si vous étiez connecté à Internet et avec quelle adresse IP, à un instant t ? Si oui, comment ?

Cependant l'opérateur qui alloue temporairement les adresses IP à ses clients enregistre toutes les traces et est en mesure de savoir exactement qui s'est connecté, avec quelle adresse IP, de même que les serveurs distants savent quelles adresses IP se sont connectées à leur service. Or la justice peut réclamer et obtenir ces données, en tout cas auprès des opérateurs français, ce qui est moins évident pour les serveurs distants.

Mais pourquoi se fatigue-t-on avec les adresses IP ?
En effet, à quoi bon s'en soucier alors qu'on s'en sort très bien sur Internet sans elles ? On se connecte à un site web ou on envoie un mail en écrivant une adresse en toutes lettres le nom qui lui correspond, et non des chiffres difficiles à retenir.
Mais si c'est possible, c'est parce que, sans le savoir, on utilise l'équivalent du répertoire pour les numéros de téléphone, c'est-à-dire un tableau qui associe chaque nom (qu'on appellera ici **adresse symbolique**, qui exprime un **nom de domaine** à distinguer de l'URL complète) à une adresse IP (numérique). Ce service de conversion s'appelle **DNS (Domain Name System)** et est assuré par un serveur dédié (en fait plusieurs), et permet notamment, s'il est correctement mis à jour, de toujours accéder à un site même si ses serveurs ont changé d'adresse IP.

2.8

Dans l'Invite de commandes de Windows, utilisez la commande ping ou la commande nslookup suivie du nom de domaine (ou un site web comme https://ping.eu/nslookup/) pour retrouver l'adresse IP des sites suivants :

Adresse symbolique	Adresse IP
https://www.laquadrature.net	185.34.33.4
https://www.afnic.fr	192.134.5.25
https://developpement-durable.gouv.fr	37.235.89.97
https://www.ecologique-solidaire.gouv.fr	37.235.89.97

Nb : les deux dernières sont identiques, développement-durable.gouv.fr est un Alias. Quand on tape cette adresse dans un navigateur, elle renvoie directement vers la seconde.

Démasquer une tentative d'arnaque grâce à l'IP

2.9

Parfois il est prudent de ne pas se fier à l'adresse symbolique et de s'intéresser à l'adresse IP. Imaginez, vous venez de recevoir un mail douteux qui dit ceci :

Cher(e) Client(e);
Nous enregistrons ce Jeudi 04 février 2016 un chèque d'un montant de **€340*.00 EUR*

*à l'ordre de MR LUSTIG VICTOR - 1 RUE ARSENE LUPIN - 39250 SHERWOOD - FRANCE
émis par *M.VERGER BENOÎT - 18 ALLEE DES TILLEULS - 64122 URRUGNE- FRANCE *

REMARQUE: Il est impératif de nous faire parvenir en répondant à ce mail (1) code de recharge PCS * de €100.00 EUR* pour vous acquitter des frais d'assurance. Dès réception et approbation du code après vérification, votre chèque vous sera expédié immédiatement. Vous le recevrez par courrier dans un (1) jour au maximum, à compter du jour de
réception du code de la recharge PCS MASTERCARD.

Christian SAINZ,
Directeur Relation Client, DHL Finance

Vous n'êtes pas bien sûr de comprendre pourquoi on vous envoie ça (pourtant c'est bien vous, Victor Lustig) mais il semble facile de gagner les 240€ promis. Que faire ?
Il faut être prudent et vérifier la provenance exacte de ce message, vérifier si tout colle bien. Voici l'entête complète de ce mail (qu'on peut faire apparaître, par ex. dans Gmail, en cliquant sur les trois points verticaux à droite de la flèche pour répondre, en haut à droite du message, puis « Afficher l'original ») :

Delivered-To: isn.pourriel@gmail.com
Received: by 10.27.14.197 with SMTP id 66csp330398wlo;
Thu, 4 Feb 2016 00:23:13 -0800 (PST)
X-Received: by 10.55.15.199 with SMTP id 68mr2039057qkp.42.1454574192794;
Thu, 04 Feb 2016 00:23:12 -0800 (PST)
Return-Path: service.dhl.international@post.com
Received: from mout.gmx.com (mout.gmx.com. [74.208.4.200])
by mx.google.com with ESMTPS id a141si9579378qkb.16.2016.02.04.00.23.12
for isn.pourriel@gmail.com
(version=TLS1_2 cipher=ECDHE-RSA-AES128-GCM-SHA256 bits=128/128);
Thu, 04 Feb 2016 00:23:12 -0800 (PST)
Received-SPF: pass (google.com: domain of service.dhl.international@post.com designates 74.208.4.200 as permitted sender) client-ip=74.208.4.200;
Authentication-Results: mx.google.com;
spf=pass (google.com: domain of service.dhl.international@post.com designates 74.208.4.200 as permitted sender) smtp.mailfrom=service.dhl.international@post.com
Received: from [192.168.1.100] ([41.191.68.245]) by mail.gmx.com (mrgmxus001) with ESMTPSA (Nemesis) id 0LrNUo-1a4NkD30Ga-01354l for isn.pourriel@gmail.com; Thu, 04 Feb 2016 09:23:11 +0100
From: "Service Expédition et Validation" service.dhl.international@post.com
To: isn.pourriel@gmail.com
Subject: CONFIRMATION DU DÉPÔT DE CHÈQUE DE BANQUE CERTIFIE

Quels sont le nom et l'adresse symbolique *apparents* de l'expéditeur ? Mais quelle est l'adresse symbolique *réelle* de son serveur mail ?
Cherchez son adresse IP dans l'entête (ou plus précisément celle de son serveur mail), puis dans un navigateur, allez sur le site https://ipgetinfo.com et cherchez des renseignements sur cette adresse. Est-elle compatible avec l'expéditeur supposé ?

Ici il faut distinguer l'adresse du prétendu expéditeur, qui correspond au destinataire affiché (« Return-Path »), service.dhl.international@post.com, qui peut facilement se falsifier et ne pas correspondre au véritable expéditeur. L'adresse du prestataire de service de boîte mail en ligne, gmx.com, dont le serveur se trouve aux Etats-Unis (mout.gmx.com : 74.208.4.200), et le serveur mail particulier, de ce prestataire, à partir duquel a véritablement été expédié le mail (mail.gmx.com : 41.191.68.245), et qui se situe en Côte d'Ivoire.
On voit qu'il y a incohérence entre l'expéditeur prétendu (qui signe le mail et s'affiche en destinataire pour une réponse) et le véritable expéditeur, il s'agit donc certainement d'une tentative d'arnaque, ce que seul l'examen des adresses IP et leur géolocalisation permet d'identifier, car les noms de domaines (gmx.com), ne sont parlants.
NB. : merci à Maxime Fourny, de l'académie de Besançon, pour le partage de ce mail (on consultera a profit ses propositions d'activités pour SNT sur M@gistere)