Rationaliser l'internet

1. Contexte :

L'adoption rapide et le déploiement à grande échelle de l'internet, qui est devenu de facto l'épine dorsale de la communication mondiale, se sont accompagnés de problèmes d'une gravité variable, allant du cyberharcèlement aux failles de sécurité en passant par les rançongiciels. L'origine de bon nombre de ces problèmes peut être attribuée à la pénurie d'adresses IPv4.

L'égalité des chances pour tous est depuis longtemps un élément important de la proposition de valeur de l'internet. Cependant, ce n'est pas une réalité, même dans la pratique de base de l'attribution des adresses. Sur la base de la population mondiale [1] et de l'allocation IPv4 actuelle [2] , les États-Unis disposent de 4,91 adresses par habitant, alors que la part de la Zambie n'est que de 0,01, soit un rapport de plus de deux ordres de grandeur et demi. La Cité du Vatican a 21,44 adresses par habitant alors que plus d'une douzaine d'entités dans le monde n'en ont aucune. Ces disparités flagrantes montrent clairement qu'il reste encore beaucoup à faire pour atteindre l'objectif.

Les efforts déployés pour surmonter les limitations de la réserve d'adresses IPv4 ont conduit à l'utilisation de l'adressage dynamique, qui est fondamentalement beaucoup plus complexe que son homologue statique. Pour une raison ou une autre, les mécanismes dynamiques continuent d'être utilisés avec l'IPv6 en l'absence de telles limitations, et personne ne semble remettre en question cette logique, peut-être en raison d'une croyance naïve commune selon laquelle l'adressage dynamique protège la vie privée et la sécurité. En réalité, cela ne s'avère vrai que pour les intrus novices. En effet, les auteurs d'infractions n'ont pas besoin de connaître l'identification spécifique d'une victime arbitraire. En revanche, lorsqu'ils ciblent des entités spécifiques telles que des écoles, des hôpitaux, des entreprises, des gouvernements, etc., la plupart de leurs adresses IP sont facilement accessibles par le biais du service DNS (système de noms de domaine), ce qui facilite les recherches. Les auteurs sérieux exploitent les faiblesses du système en se cachant derrière des adresses fictives qui peuvent être modifiées arbitrairement lorsqu'ils lancent leurs attaques.

Pire encore, la pratique des adresses dynamiques a rendu si difficile l'analyse médico-légale du trafic Internet qu'elle a justifié la surveillance de masse sans discernement par les forces de l'ordre au nom de la prévention de la criminalité. Puisque rien n'empêche une autre partie de faire de même, si elle est équipée, il ne reste en fin de compte que peu, voire pas du tout, de vie privée pour les individus ordinaires ! Ce sujet est devenu très controversé et alambiqué [3] .

Prévu pour remplacer l'amélioration de l'IPv4, l'IPv6 a eu la grande surprise de ne pas être rétrocompatible, ce qui a rendu la transition difficile et coûteuse. Il a fallu créer le protocole provisoire Dual-Stack [4] qui a augmenté les coûts sans vraiment atténuer le handicap initial.

La connectivité de bout en bout a toujours été imposée comme le premier critère de toute proposition d'amélioration de l'internet, mais l'effet cumulatif des défis susmentionnés a conduit à un CDN (Content Delivery Network - le modèle d'exploitation de l'internet actuellement prédominant) caractérisé par une architecture maître-esclave qui entrave en fait la communication directe d'égal à égal entre les utilisateurs finaux, même à l'intérieur d'une communauté locale.

Une autre partie de la proposition de valeur initiale de l'Internet était de libérer les systèmes de communication publics du monopole de quelques grands fournisseurs de télécommunications et de la réglementation des agences gouvernementales. Cependant, des décennies plus tard, le service Internet est désormais segmenté en plusieurs secteurs d'activité, chacun étant desservi par un seul conglomérat multinational dominant (et quelques concurrents plus petits) qui est si puissant et influent qu'il est en mesure d'échapper aux réglementations tout en minimisant la responsabilité des problèmes qu'il crée.

Dans le même temps, l'implication croissante des gouvernements souverains du monde entier dans les opérations quotidiennes de l'internet a fait l'objet de nombreuses critiques, car elle conduit à la fragmentation de l'internet en un Splinternet [5]. Le fait est que les FAI (fournisseurs d'accès à l'internet) ont divisé l'architecture de l'internet en de nombreux AS (systèmes autonomes) [6] nécessitant le protocole BGP (Border Gateway Protocol) [7] pour les interconnecter. Le Splinternet géopolitique diviserait un réseau de communication mondial à couche unique en fragments nationaux (environ

195 au total) [8], tandis que les AS ont déjà créé des couches (actuellement environ 76 000 et en augmentation) [9] de réseaux sphériques, chacun enveloppant le globe entier comme une couche complète de pelures d'oignon. Dans un certain sens, le nombre de ces couches de "réseaux-oignons" est presque deux ordres de grandeur et demi plus élevé que celui des fragments potentiels de Splinternet. Ce contraste est vraiment stupéfiant, même avant de reconnaître que le nombre d'AS possibles est le même que le pool d'adresses IPv4 de 32 bits ! [10]. La critique du Splinternet est peut-être une tactique visant à détourner l'attention de l'Onion-net.

Compte tenu de tout ce qui précède, il n'est pas surprenant qu'il faille autant de temps pour diagnostiquer et comprendre l'ampleur d'un événement Internet d'urgence, et encore plus dans le cas d'un piratage malveillant - des jours, des semaines, des mois ou même plus longtemps - pour commencer à spéculer sur l'auteur d'une cyber-attaque majeure. En comparaison, le réseau téléphonique public commuté (RTPC) traditionnel est capable de localiser l'appelant avant même qu'il ne réponde à l'appel.

En résumé, l'incapacité de la conception originale de l'internet basée sur l'IPv4 à identifier de manière explicite et unique chaque personne dans le monde a conduit à divers remèdes dynamiques. Malheureusement, ces remèdes ont également fourni le camouflage parfait pour les auteurs malveillants désireux d'attaquer des utilisateurs légitimes mais vulnérables. Bien que la nouvelle version IPv6 dispose de plus d'adresses qu'il n'en faut pour identifier tous les IoT (Internet des objets), les schémas provisoires IPv4 se perpétuent. En outre, l'installation d'IPv6, contrainte d'utiliser le schéma Dual-Stack en raison de l'absence de compatibilité ascendante, est plus compliquée et plus coûteuse que l'IPv4 pur, ce qui fait que les régions en développement ont du mal à adopter l'IPv6. Ces complexités augmentent la vulnérabilité des réseaux aux cyberattaques. Néanmoins, il est hors de question de remplacer rapidement un grand système utilisé en permanence comme l'internet, surtout dans son intégralité.

2) Exigence :

Pour sortir de cette impasse, une solution réaliste doit pouvoir coexister avec l'environnement actuel tout en évoluant vers un système à long terme. L'approche idéale consisterait à introduire un système qui se comporte comme une partie du système existant - sans perturber les opérations en cours - mais qui a la capacité d'évoluer vers un réseau

superposé fonctionnant indépendamment de l'installation de base, tout en conservant des interfaces sans lien de dépendance entre les deux pour assurer l'interopérabilité et l'intégrité globale du service. Ces réseaux évolueraient progressivement vers deux systèmes fonctionnant en parallèle, utilisant la même technologie, mais suivant des disciplines opérationnelles différentes pour fournir des services comparables. Cela permettrait aux utilisateurs finaux d'expérimenter personnellement et de comparer les avantages et les inconvénients des deux systèmes afin de choisir en connaissance de cause la configuration à long terme qu'ils préfèrent.

3. Solution :

Heureusement, un schéma compact [11] capable de résoudre la plupart des problèmes évoqués jusqu'à présent a été identifié. L'approche de base de ce schéma consiste à utiliser le bloc de réseau 240/4 réservé depuis longtemps dans le bloc de construction du CDN existant, CG-NAT (Carrier Grade - Network Address Translation) pour établir une nouvelle installation, appelée SPR (Semi-Public Router), afin de superposer l'infrastructure Internet actuelle. Aucune nouvelle technologie n'est requise dans le cadre d'un tel déploiement au fil du temps.

Disposant de suffisamment d'adresses statiques pour identifier chaque utilisateur, un SPR n'a pas besoin de DHCP (Dynamic Host Configuration Protocol), ce qui fait que les IAP n'ont pas d'adresses allouées à attribuer. Comme le DNS dégénère essentiellement en une base de données quasi-statique équivalente aux pages blanches de la téléphonie électronique et que l'AS et le BGP ne sont plus nécessaires, ce nouvel environnement internet est très simplifié.

Pour utiliser le bloc de réseau 240/4 qui est resté si longtemps "réservé", il peut être difficile de trouver un équipement facilement disponible pour tester la capacité du dispositif et vérifier la performance du réseau. En outre, cet équipement doit être concis, peu coûteux et d'une courbe d'apprentissage minimale afin d'encourager le plus grand nombre possible de parties intéressées à se lancer dans la transition proposée.

Les paragraphes suivants décrivent l'équipement et le processus de base nécessaires à la mise en place d'un banc d'essai pour les expériences et les démonstrations. Les compétences et l'expérience acquises lors de ces

dernières peuvent ensuite être mises à profit pour faciliter le déploiement effectif du SPR.

. **Instrument terminal :**

Xubuntu [12] V18.04.1 a été identifié comme le candidat OS (système d'exploitation) le plus pratique parce qu'il peut assumer simultanément deux adresses IP sur le même PC portable hôte (ordinateur personnel). En d'autres termes, chaque PC ainsi équipé se comporte comme deux IoT partageant le même port réseau matériel, à savoir un client commun adressé par DHCP et un client statique. Tous deux peuvent porter l'adresse IPv4 ou 240/4. Une paire d'IoT DHCP IPv4 sur ces PC peut établir la connectivité physique entre eux via le processus de mise en réseau conventionnel. Ensuite, les IoT statiques à adresse 240/4 sur la même paire de PC peuvent vérifier les caractéristiques de transmission dans l'environnement 240/4. Sans modification de la configuration matérielle ni redémarrage des PC, ce test en deux étapes garantit que le support est prêt à transporter des paquets avec n'importe quelle adresse IPv4 dans l'une ou l'autre catégorie. En outre, ces PC peuvent être utilisés avec un nouvel IoT via ce support pour vérifier sa compatibilité avant de le déployer sur le terrain.

. **Simulateur de réseau:**

Un banc d'essai compatible 240/4 sert de tissu de base pour qualifier les appareils compatibles et vérifier leurs performances de transmission.

A. Pour un point de départ définitif, un RG (Routing/Residential Gateway) devrait être rendu totalement capable de 240/4 en installant le firmware OpenWrt [13] V19.07.3, ou plus, qui prend en charge une longue liste de RG commerciaux. Cela permettra d'établir des réseaux locaux (Local Area Networks) et des réseaux domestiques (Home Area Networks) sur place qui serviront à la fois aux IoT traditionnels et à ceux qui utilisent des adresses 240/4, tout en se comportant comme des clients DHCP 240/4 sur l'internet.

B. Pour fournir une structure de transmission de base entre les locaux (représentés par les GR ci-dessus) fonctionnant comme un SPR, les commutateurs gérés intelligents D-Link de la série DGS-1210 supportés par OpenWrt [14] sont de bons candidats.

Pendant qu'un SPR se développe, il forme un réseau superposé qui dessert essentiellement les mêmes locaux avec les mêmes fonctions que le tissu CG-NAT existant, sauf que le schéma de routage par défaut devient hiérarchique. Ce processus peut être répliqué pour finalement recouvrir un cluster CG-NAT entier. Ensuite, plusieurs grappes CG-NAT peuvent être desservies à partir d'un seul SPR en tirant pleinement parti de la taille du bloc réseau 240/4, qui est 64 fois supérieure à celle d'un bloc réseau 100,64/10, ce qui fixe la limite de la capacité d'une grappe CG-NAT sans réaffectation dynamique. En fonction de la taille de la population à desservir, un RAN (réseau régional) [15] peut se composer d'un ou de plusieurs SPR.

4. Conclusion :

Étant donné que le bloc de réseau 240/4 a été officiellement désigné comme "réservé pour une utilisation future" ou "expérimental" pendant de nombreuses années, des questions se sont naturellement posées quant à son utilisation. Des conglomérats commerciaux multinationaux ont été signalés comme utilisant effectivement le bloc de réseau 240/4 à diverses fins, sans aucune annonce [16]. Le fait qu'il ait fallu des efforts pour découvrir de telles activités indique que l'utilisation du bloc 240/4 ne perturbe pas et ne perturbera pas les opérations Internet existantes. Le bloc de réseau 240/4 est donc un véhicule idéal pour déployer le SPR proposé.

En utilisant des adresses statiques, le RAN rationalisera le fonctionnement de l'internet grâce à un routage hiérarchique qui permettra au grand public de bénéficier d'une communication d'égal à égal, à l'abri de la domination des conglomérats commerciaux multinationaux. La nature statique du système d'adressage permet au RAN d'être plus déterministe que l'internet actuel basé sur le CDN, et donc plus robuste contre les cyber-intrusions.

Pour plus d'informations, il existe un livre blanc en ligne [17] qui analyse cette proposition d'un point de vue plus commercial.

Références :

[1] Pays du monde par population ; https://www.worldometers.info/world-population/population-by-country/

[2] Liste des pays par allocation d'adresses IPv4 : https://en.wikipedia.org/wiki/List_of_countries_by_IPv4_address_allocation

[3] État des vulnérabilités en matière de cybersécurité https://blo.apnic.net/2021/02/03/the-internet-of-trash/

[4] IPv6 : https://en.wikipedia.org/wiki/IPv6

[5] Splinternet https://en.wikipedia.org/wiki/Splinternet#:~:text=The%20splinternet%20(également%20référé%20à,religion%2C%20et%20intérêts%20nationaux%20divergents.

[6] Système autonome https://en.wikipedia.org/wiki/Autonomous_system_(Internet)

[7] Protocole de passerelle frontalière https://en.wikipedia. o rg/wiki/Border_Gateway_Protocol

[8] Pays dans le monde https://www.worldometers.info/geography/how-many-countries-are-there-in-the-world/#:~:text=There%20are%20195%20countries%20in,and%20the%20State%20of%20Palestine.

[9] Nombre d'AS actuels https://thyme.apnic.net/current/data-summary

[10] Numéros de systèmes autonomes https://www.arin.net/resources/guide/asn/

[11] Brevet américain n° 11,159,425 https://image-ppubs.uspto.gov/dirsearch-public/print/downloadPdf/11159425

[12] Xubuntu
https://xubuntu.org/

[13] OpenWrt
https://openwrt.org/toh/start?toh.filter.supportedcurrentrel=22.03%7C23.05

[14] Commutateurs intelligents de la série D-Link DGS-1210
https://www.dlink.com/us/en/products/dgs-1210-series-gigabit-smart-plus-switches

[15] Simulateur de réseau régional
https://www.avinta.com/gallery/RegionalAreaNetworkSimulator.pdf

[16] Utilisation du 240/4 à l'improviste
https://labs.ripe.net/author/qasim-lone/2404-as-seen-by-ripe-atlas/

[17] Réorganiser l'Internet :
https://www.avinta.com/gallery/RevampTheInternet.pdf

Terminologie, abréviation et acronyme :

. AS : Système autonome

. BGP: Gateway Protocol (protocole de passerelle

CDN: Content Delivery Network (réseau de diffusion de contenu)

. CG-NAT : Carrier Grade Network Address Translation (traduction d'adresses de réseau de qualité transporteur)

. DHCP : protocole de configuration dynamique de l'hôte

. DNS : Système de noms de domaine

. Double pile : Un environnement de réseau qui prend en charge l'utilisation simultanée des adresses IPv4 et IPv6.

. HAN: Home Area Network (réseau sur placepour les parties privées/résidentielles)

. IAP: Fournisseur d'accès à Internet

. IoT : Internet des objets

. IPv4 : Protocole Internet version 4

. IPv6 : Protocole Internet version 6

. LAN : Local Area Network (Réseau local utilisé par les institutions)

. OS : Système d'exploitation

. PC : Ordinateur personnel

. PSTN : Public Switched Telephone Network (réseau téléphonique public commuté)

. RAN: Réseau régional

. RG : Routage/Passerelles

. SPR : Routeur semi-public

. 240/4Netblock : Pool d'adresses IPv4 allant de 240.0.0.0 à 255.255.255.255, représentant environ 256 millions (256M) ou un quart de milliard (0.256B) d'adresses qui n'ont pas été utilisées officiellement depuis 1981-09 parce qu'elles ont été désignées comme "expérimentales" ou "réservées" pour une "utilisation future".

ahttps://www.ian.org/assignments/ipv4-address-space/ipv4-address-space.xhtml