Société pour l'attribution des noms de domaine et des numéros sur Internet

Rapport sur l'innovation technologique en matière d'identificateurs

Le 15 mai 2014 – Version finale

Table des matières

1. Introduction

Le panel sur l'innovation technologique en matière d'identificateurs (ITI) s'est vu confier par la Société pour l'attribution des noms de domaine et des numéros sur Internet (ICANN) les objectifs suivants :

1. élaborer une feuille de route technologique pour le système des noms de domaine (DNS) et d'autres identificateurs ;

2. élaborer des recommandations en matière de meilleures pratiques et des systèmes de référence ;

3. orienter du point de vue technologique les opérations, la sécurité, la politique et les fonctions techniques de l'ICANN ;

4. dialoguer avec la communauté de l'ICANN et le public sur des questions d'ordre technologique.

Le panel, présidé par Paul Mockapetris, a été sélectionné de septembre à octobre 2013. Tous ses membres y ont participé à titre individuel, leur affiliation figurant ici uniquement à des fins d'identification :

- Jari Arkko, président, Groupe de travail de génie Internet (IETF)
- Rick Boivie - Centre de recherche IBM Thomas J. Watson
- Anne-Marie Eklund-Löwinder — responsable de la sécurité, Internet Infrastructure Foundation (IIS)
- Geoff Huston, chef de l'équipe scientifique du Centre d'information de réseaux d'Asie-Pacifique
- James Seng — PDG, Zodiac Holdings
- Paul Vixie — PDG, Farsight Security
- Lixia Zhang — responsable de la chaire d'informatique Postel à l'Université de Californie, Los Angeles

Le groupe s'est réuni en personne à l'occasion de l'IETF Vancouver (novembre 2013), à la réunion de l'ICANN à Buenos Aires (novembre 2013) et dans les bureaux de l'ICANN à Los Angeles (janvier 2014). La réunion de Buenos Aires était ouverte au public et un résumé des activités du panel a également été présenté dans deux séminaires en ligne en janvier 2014. Les discussions par courrier électronique et autres ont complété ces échanges. La version préliminaire des rapports a été disponible pour consultation publique à partir du mois de février 2014.

Le président tient à remercier le panel pour ses réflexions et ses idées, ainsi que l'ICANN pour son soutien. Un grand merci aussi à Elise Gerich et à Alice Jansen, de l'ICANN, pour leurs idées et leur soutien au travail du panel.

2. Panel de stratégie

Le nom du panel n'a pas été choisi au hasard. Le champ d'application de son travail a été étendu au-delà du seul domaine du DNS pour tenir compte de l'importance croissante des identificateurs de toutes sortes pour l'Internet, ainsi que du rôle de l'ICANN dans la gestion d'autres identificateurs. Une liste partielle du portefeuille actuel de l'ICANN comprend :

- les noms de domaine
- les numéros du système autonome (AS)
- les adresses Internet IPv4
- les adresses Internet IPv6
- les adresses multicast
- les numéros de port
- les numéros de protocole
- le registre des identificateurs uniformes de ressources (URI)
- la base de gestion des informations (MIB)
- la base de données des fuseaux horaires

Cependant, cette extension de la portée du travail du panel s'est accompagnée d'une réduction de moitié des délais prévus, qui ont passé d'un an à environ six mois. C'est la raison pour laquelle l'examen est plus focalisé sur le DNS que ce qu'on aurait souhaité.

Pour compenser, le panel a adopté les principes suivants :

- essayer de documenter toutes les idées envisagées, mais mettre l'accent sur quelques-unes d'entre elles ;
- identifier des tendances qui s'imposent (par exemple l'expansion de l'Internet, les tendances en matière d'architecture de processeur) ;
- identifier les besoins « brûlants » ;
- éviter de se concentrer sur les « sentiers battus » (par exemple le déploiement de DNSSEC, les stratégies existantes pour gérer les collisions) et chercher de nouvelles idées.

L'objectif central du panel est de fournir les éléments nécessaires au processus de planification stratégique de l'ICANN. Bien que le panel ait analysé des notions liées aux besoins opérationnels de l'ICANN, il ne s'est pas limité à des idées qui seraient mises en œuvre par l'ICANN. La mise en œuvre de bon nombre des idées discutées ici relèverait naturellement de l'IETF ou d'autres instances. Certaines de ces réflexions soulèvent des questions politiques que nous n'avons pas abordées et dont nous avons tout simplement signalé l'existence.

Finalement, en raison de l'énorme activité constatée dans l'espace des identificateurs, le panel s'est tout simplement limité à échantillonner cet espace. Le lecteur ne doit pas supposer que nous connaissions toutes les activités en cours, ou que les idées qui ne sont pas abordées ici sont moins importantes.

3. Feuille de route

Les identificateurs restent une question sensible pour la communauté Internet. À court terme, les nouveaux domaines de premier niveau (TLD) seront en ligne. Votre compte Facebook cherchera à devenir votre authentification unique pour accéder à l'Internet –à l'instar du compte Google. À long terme, la communauté des chercheurs envisage beaucoup de projets différents dont, entre autres, les réseaux basés sur le contenu (CCN), les réseaux basés sur l'information (ICN) et les réseaux fondés sur les objets nommés (NDN). Si la communauté de chercheurs n'arrive pas à se mettre d'accord pour accorder un nom à ce nouveau domaine, elle reconnaît pourtant que le contenu doit être identifié par son nom, et non pas par son adresse ou son emplacement, et que la mise en cache devrait être opportuniste. D'autres propositions insistent sur le fait que les noms plats représentent l'avenir et que l'auto-certification des noms devrait être à la base de tout nouveau système.

Les identificateurs sont au cœur de tous les réseaux dans la mesure où ils servent à identifier certaines de leurs composantes par rapport à toutes les autres composantes des réseaux. En outre, les réseaux modernes ne sont pas constitués comme un seul domaine homogène mais sont construits à partir de l'amalgame d'un certain nombre de technologies, d'où la nécessité de mettre en correspondance les différents univers d'identification. Cette fonction de cartographie est effectuée de différentes manières. Dans le contexte de l'Internet, l'un des univers d'identification les plus visibles est celui des noms de domaine, un espace de noms structuré hiérarchiquement. Cet espace de noms est associé à une fonction de cartographie qui permet de mettre en correspondance les noms domaines avec d'autres d'identificateurs (comme les adresses IP, par exemple). Lors de l'élaboration d'une feuille de route pour les identificateurs, il faut bien faire la distinction entre l'univers des identificateurs et la fonction de cartographie, afin d'établir des feuilles de route pour chacun de ces éléments.

Dans l'Internet actuel, le panel a identifié plusieurs facteurs qui contribuent à élargir l'utilisation du DNS, ainsi que certains autres qui ont tendance à la restreindre. Ces facteurs ne sont pas d'ordre technique et le conflit semble moins associé à une question d'élégance -ou de tout autre vertu- qu'à une nature plutôt darwinienne.

Facteurs d'expansion actuels

- Le DNS bénéficie d'un avantage hérité, lié au fait qu'il existe dans chaque dispositif connecté à Internet. La simple croissance de la base existante va conduire à une expansion de son utilisation. Par exemple, une application qui veut franchir les pare-feux et être mise en cache sur l'Internet se retrouve avec le DNS comme un élément existant.
- Les nouveaux TLD vont tenter de monétiser leurs marques. Alors que le scepticisme est de mise parmi la communauté technique, plus de mille nouvelles marques lutteront pour se tailler une place dans le marché avec, à la clé, des innovations probables et plusieurs surprises.
- De nouvelles fonctionnalités, comme les extensions de sécurité du système des noms de domaine (DNSSEC) ou l'authentification d'entités nommées basée sur le DNS (DANE) pourraient promouvoir l'utilisation du DNS.

- De nouvelles données dans le DNS pourraient élargir son utilisation, notamment lorsqu'elles sont combinées à DNSSEC pour garantir leur authenticité. Un membre du panel a recommandé l'inclusion d'informations telles que l'« anniversaire », le nom du bureau d'enregistrement et l'« intervalle depuis le changement de la délégation » parmi les données liées à la réputation d'un domaine. D'autres propositions visent à utiliser le DNS comme un registre de blocs d'adresses, de systèmes autonomes, etc. L'ICANN a restreint l'utilisation de certaines étiquettes dans les noms de domaines et un registre de ce type en temps réel pourrait s'avérer approprié, notamment lorsque les spécifications viennent en plusieurs alphabets. Dans la pratique, ces bases de données peuvent être publiques ou privées.
- L' « Internet des objets » (IOT) représente différentes choses pour les différentes personnes, mais inclut typiquement un nombre extrêmement important d'unités dans une ou plusieurs bases de données distribuées gigantesques. Le DNS a été proposé comme une composante de base de plusieurs architectures et prototypes IOT, autant au niveau du DNS public que des bases de données DNS privées. Le panel aurait souhaité avoir le temps d'explorer cette question en profondeur, en recommande un examen plus détaillé et considère que le DNS pourrait très bien y jouer un rôle.

Facteurs de contraction actuels

- Le DNS est la norme héritée mais cela constitue aussi un handicap en ceci que le DNS-logic intégré dans les points d'accès WIFI, les lignes numériques d'abonnés (DSL) et les modems-câbles, les pare-feux, les routeurs et la base logicielle de l'Internet limite souvent le champ d'utilisation du DNS et freine l'innovation. Les mises en œuvre du DNS sont souvent loin d'être complètes, actualisées ou conformes aux normes. Ces problèmes ont freiné le déploiement de DNSSEC et ont rendu problématique la mise en œuvre de nouveaux types ou fonctions du DNS. Cela a conduit à des pratiques destinées par exemple à limiter son utilisation aux seules adresses et enregistrements textuels (TXT). Cette immuabilité n'est pas unique au DNS.
- Le contrôle (« owning ») de la fenêtre de recherche et/ou de l'espace d'identification revêt un intérêt commercial. L'intérêt porte ici sur le fait de connaître la première tentative saisie par l'internaute en toute liberté et de la cacher de l'Internet ouvert. Le panel a constaté une tendance vers des dispositifs codés en dur pour un service DNS spécifique, ainsi que des extensions propriétaires, comme une voie vers la balkanisation.
- Les utilisateurs préfèrent une interface plus puissante. Plutôt que de saisir les noms DNS, les utilisateurs et les applications utilisent souvent la recherche et d'autres mécanismes pour obtenir une information en particulier. Par exemple, la barre des adresses universelles (URL) dans les navigateurs est, à l'heure actuelle, un outil de recherche. Actuellement, l'interface utilisateur la plus courante est le dispositif mobile, ce qui ne favorise pas la saisie. La reconnaissance vocale et d'autres types d'intelligence artificielle (IA) dans la barre du navigateur entraînent des incompatibilités entre les différents fournisseurs. Par exemple, une expérience tentée par le panéliste Geoff Huston (voir contribution) a montré que la recherche des mots « Geoff.Huston » dans plusieurs navigateurs donnait lieu à des résultats NON cohérents entre

les fournisseurs. Ce manque de cohérence peut être tolérable dans les recherches faites à l'aide d'un navigateur, où l'utilisateur est censé vérifier les résultats, mais peut être dangereux lorsqu'il s'agit de fichiers de configuration des systèmes — dont un des problèmes est celui de la collision.

Le panel a l'impression que si l'utilisation du DNS tend à disparaître de l'interface utilisateur, il n'en reste pas moins une infrastructure de base. À titre d'analogie, on peut dire que le DNS n'est pas comparable au livre papier face à l'essor du livre électronique, mais plutôt à un ensemble d'instructions informatiques auxquelles il est possible d'accéder par le biais de langages de plus haut niveau.

Les opinions sont divergentes quant à savoir s'il est possible ou souhaitable de rechercher une renaissance ou une restructuration du DNS. Les aspects technologiques sont abordés dans la section « fondements du DNS » de ce rapport. Une question politique se pose : celle de savoir si l'ICANN devrait essayer de préserver et d'élargir le système des noms de domaine (DNS). Si oui, comment peut-on obtenir une architecture cohérente, basée sur les différents points de vue des unités constitutives de l'ICANN, de l'IETF (où serait fait probablement le travail) et des autres parties de l'Internet ?

Le long terme

Parmi les idées à développer à long terme on retrouve le modèle de réseau fondé sur les objets nommés (NDN). Les idées clés de ce modèle sont l'accès au contenu par le nom, l'authentification numérique partout, la mise en cache opportuniste et un régime de flux dans lequel les demandes de contenu et les réponses suivent la même voie. Pour le routage de requêtes, on dit parfois que ce modèle utilise simplement une hiérarchie de noms pour que les préfixes les plus longs puissent trouver une correspondance dans les décisions de routage, ce que les sceptiques trouvent difficile à faire évoluer. Quoi qu'il en soit, des essais au niveau du logiciel, du matériel et du réseau ont été mis en œuvre. Les applications les plus évidentes de ce modèle concernent la distribution de contenu, mais ses défenseurs affirment qu'il est performant pour le contrôle de processus, les réseaux automobiles, etc.

D'une certaine façon, le DNS a été la première alternative des opposants à la table rase pour éviter le "tout ICN" (réseau basé sur l'information), comme c'est le cas d'autres approches plus récentes [Fayazbakhsh 2013] qui essaient de préserver seulement les parties les plus importantes du modèle ICN. La beauté ici est dans l'œil de celui qui regarde.

Le DNS récupère les données par nom. Il ne tente pas de router par nom mais utilise à la place la couche d'adressage Internet pour rendre le contenu trouvable. Ce schéma montre ce que pour certains constitue le principal problème d'évolutivité pour le modèle ICN. Le DNS est devenu tristement célèbre comme moyen de tunneliser des contenus vidéo [Kaminsky 2004] et comme canal caché d'accès illicite à travers des requêtes DNS effectuées avant authentification par certains points d'accès WIFI. (Si on cherche « DNS tunneling » sur Google on obtient environ 1 620 000 résultats.)

L'ICN établit des correspondances par le préfixe le plus long et compte des sélecteurs qui permettent le transport de contenu multimédia, des fonctions prévues dans la section requête de la spécification originale du protocole DNS mais qui n'ont jamais été développées.

En tout cas, en supposant que l'on puisse faire des paquets DNS plus grands et ajouter certains champs de requête supplémentaires, les services de contenu pourraient être reproduits dans le DNS. La correspondance des requêtes et des réponses authentifiées de l'ICN peut être la meilleure façon d'éviter les attaques par amplification de DNS.

Pour conclure, on pourrait imaginer un schéma NDN à la place du DNS, qui commencerait probablement comme un super-ensemble de fonctions DNS dont le basculement total prendrait des années ou des décennies. Toute tentative visant à améliorer l'architecture du DNS devrait pouvoir emprunter librement des éléments du modèle NDN.

Le modèle ICN est loin d'être le seul modèle pour l'avenir, il s'agit tout simplement d'un des plus développés. Le panel considère qu'il est toujours utile d'essayer de s'abstraire par rapport aux principes de base et de se pencher ensuite sur la composition. [Ghodsi2011] en est un bon exemple, pour la façon dont il relie le nom, l'ID du monde réel et l'infrastructure de gestion de clés publiques (PKI).

Plus récemment, l'accent a été mis sur la distribution du contrôle [Newyorker 2014] et la confidentialité, le système Namecoin étant l'exemple le plus connu. L'infrastructure de gestion de clés publiques (PKI) qui existe aujourd'hui dans l'Internet représente une ressource pour la surveillance à grande échelle, et de ce fait un problème pour la vie privée. Un mélange d'objets auto-certifiants avec une option PKI, ou encore de systèmes parallèles de PKIs et de pair à pair (P2P) pourrait être la réponse. Le panel ITI n'a pas exploré cette piste mais la trouve très intéressante.

4. Questions opérationnelles

Plusieurs questions se posent par rapport aux opérations quotidiennes de l'ICANN. Elles tournent essentiellement autour de la racine.

4.1. Renforcement de la racine

Compte tenu de l'importance de l'infrastructure de la racine, le panel a reçu plusieurs suggestions lui recommandant de se pencher sur les technologies « Trusted computing » (informatique de confiance). Le panel considère qu'il pourrait y avoir intérêt à appliquer ce type de technologie dans les systèmes utilisés pour modifier et signer la racine, mais a décidé qu'il était davantage prioritaire de se pencher sur l'amélioration de la distribution des données signées plutôt que sur du matériel standard. Les révélations de Snowden ont signalé du doigt certains problèmes de sécurité au niveau du matériel qui peuvent ne pas avoir été considérés au moment de la conception des systèmes actuels, comme c'est le cas, entre autres, des infections du BIOS et des logiciels espions dans le disque dur [Spiegel 2014].

4.2.Réplication

Le DNS a toujours eu deux mécanismes complémentaires pour la distribution des données : la réplication planifiée des zones et les requêtes sur demande. Du point de vue d'un élément individuel de données DNS, un enregistrement de ressource (RR) commence à sa source première, dans une zone ; voyage ensuite avec cette zone dans un ou plusieurs transferts de zone ; et arrive à destination lorsqu'il est récupéré par une requête.

Par exemple, la zone racine est générée par l'ICANN en partenariat avec Verisign et le département du commerce des États-Unis, puis distribuée à tous les serveurs racine à travers les transferts de zone. Sur le plan conceptuel, cette distribution, comme d'ailleurs la distribution de toute autre zone dans le DNS, peut être faite par n'importe quel mécanisme : des livraisons par bandes magnétiques et Federal Express (FedEx), des transferts de fichiers via le protocole de transfert de fichiers (FTP) ou Rsynch, ou encore mieux par transfert incrémental de zone, où seules les modifications par rapport à une version précédente sont transférées, au lieu de toute la zone. Des copies peuvent être soit envoyées par notification DNS, soit récupérées à l'aide d'une stratégie d'interrogation destinée à identifier les modifications. Les transferts de zone peuvent être sécurisés à travers le protocole de signature de transaction du DNS (TSIG) et / ou par d'autres protocoles de transport, par exemple, le protocole de sécurité IP (IPsec), le protocole de transfert hypertexte sécurisé (HTTPS), etc. Il y a des centaines d'instances de serveurs racine avec des copies de la zone racine.

Lorsque les utilisateurs veulent accéder à des données dans la zone de racine, ils envoient des requêtes à la racine. Les requêtes sont acheminées par deux mécanismes : dans un premier moment, l'adresse IP de destination dans la requête identifie un ensemble de serveurs racine qui partagent une adresse anycast commune ; ensuite, le système de routage décide quel serveur dans l'ensemble anycast recevra effectivement la requête. Ce schéma résulte de l'évolution d'une configuration initiale de 3 serveurs racine avec des adresses unicast, qui s'est étendue par la suite à 13 organisations de serveurs racine mettant en place la répartition de charge en grappes de serveurs, pour arriver finalement au schéma actuel (avec des étapes intermédiaires). Pour le dire de façon simplifiée : les « 13 serveurs racine » sont en réalité « 13 organisations de gestion des serveurs racine » qui transmettent la zone à des centaines ou des milliers de serveurs individuels[1]. Nous n'avons que 13 organisations de serveurs racine et nous utilisons anycast parce que cela était beaucoup plus facile à faire que de supprimer la limitation de taille des paquets DNS du protocole de datagramme utilisateur (UDP). Il existe aussi d'autres problèmes de taille liés à l'incorporation d'adresses IPv6. Le DNSSEC peut éventuellement assurer la sécurité de l'acheminement allant du serveur racine vers l'utilisateur.

Au fil des années, les serveurs racine ont fait l'objet d'attaques, la plupart étant du type déni de service distribué (DDOS). Pour qu'une attaque de ce genre contre un utilisateur particulier soit couronnée de succès, elle doit perturber les requêtes vers toutes les adresses anycast des 13 organisations de serveurs racine. La perturbation d'un sous-ensemble provoquera le ralentissement des performances pendant que le responsable identifie quels sont les serveurs racine à éviter. La perturbation peut mettre hors service le serveur ou le chemin du réseau vers le serveur, en général avec une surcharge. Par exemple, pendant une de ces attaques, les utilisateurs en Californie ont pensé que le serveur racine était hors

[1] À l'heure actuelle, deux des organisations de serveurs racine sont exploitées par la même entité, Verisign.

service, alors qu'à Stockholm les utilisateurs ont constaté exactement la situation contraire. Les organisations gestionnaires des serveurs racine ont répondu à une menace récente du collectif de pirates informatiques Anonymous en grande pompe, déployant davantage de bande passante et de serveurs.

Bien entendu, l'attaque ne doit pas forcément être adressée à la constellation du serveur racine ; elle peut être adressée à la connexion Internet de l'utilisateur. Bien que limitée en dégâts, le rapport de forces entre un réseau zombie et une entreprise est souvent favorable à l'attaquant, y compris s'il s'agit d'importantes entreprises.

Certains membres du panel ont recommandé aux entreprises de distribuer en interne des copies de la racine **et de toute autre zone critique,** de sorte que lors d'une attaque, le fonctionnement normal puisse se poursuivre, au moins pour le DNS. L'ICANN facilite à toutes les organisations l'obtention d'une copie de la zone racine, et avec un petit peu plus de travail, leur propose de devenir une instance du serveur racine L géré par l'ICANN. C'est aussi une bonne idée pour une entreprise de devenir autosuffisante par rapport au DNS et de ne pas être confrontée au risque de ne plus pouvoir accéder à des serveurs externes ou à des contraintes imposées, intentionnellement ou non par un registre, un bureau d'enregistrement, des opérateurs de serveurs racine, etc.

Grâce à DNSSEC, nous avons un moyen de distribuer une zone qui peut être vérifiée à l'aide de signatures numériques intégrées. Le panel considère que ce principe peut être encore développé, par exemple en protégeant la délégation et les données de type glue. Il peut également être possible d'éliminer ou de réduire les organisations de serveurs racine et les données d'adressage. Un procédé décrit en détail par le panéliste Paul Vixie est inclus dans la section Contributions de ce rapport.

Il existe aussi des aspects politiques importants. Le fait qu'il n'y ait que 13 organisations de serveurs racine provoque chez certains pays le sentiment d'être laissés à l'écart, même s'ils sont en mesure d'accueillir autant d'instances du serveur racine L de l'ICANN qu'ils seraient prêts à accepter (sans compter que plusieurs autres organisations de serveurs racine sont prêtes à élargir leurs constellations anycast). Essayons donc de faire disparaître le problème.

Il convient de noter qu'il n'existe aucune nécessité technique de remplacer le système de serveurs racine existant comme certains le souhaitent ; essayons simplement de faire en sorte que la réplication de la racine soit plus facile et donnons l'exemple aux autres zones.

4.3. Zone de contrôle partagé

Dans la section précédente, nous avons discuté des sensibilités politiques qui sont à l'origine du fait que les pays veuillent gérer une organisation de serveur racine. Ces préoccupations peuvent être bien fondées ou pas, il n'en demeure pas moins que la gestion actuelle de la racine est basée aux États-Unis et soumise à la juridiction des États-Unis.

De manière générale, la racine est mise à jour suivant la séquence ci-dessous :

- l'ICANN reçoit des demandes de mise à jour des TLD et vérifie qu'elles ne comportent pas d'erreurs,
- l'ICANN soumet les modifications au département du commerce,
- l'ICANN envoie les modifications approuvées à Verisign,
- Verisign génère une racine signée et la distribue.

Existe-il un moyen technique envisageable pour partager le contrôle sur la racine ? Il y a plusieurs théories en la matière. Il existe une théorie qui affirme que les données doivent avoir N signatures multiples. Puis M / N signatures sont nécessaires pour authentifier les données. Bien sûr, il y a des querelles à propos de la taille de M et de N, ainsi que sur la question de savoir s'il est nécessaire ou souhaitable d'adopter une cryptographie différente.

Nous n'avons pas ici l'intention de plaider en faveur d'un système spécifique, mais nous pensons qu'une bonne conception pourrait déjà permettre la mise en place d'un processus politique pour décider comment le contrôle d'une zone spécifique pourrait être partagé. À notre avis, il faudrait créer une boîte à outils pour le contrôle partagé de zone, non seulement pour la racine, mais aussi pour d'autres problèmes de coordination de zone. Le panel fait remarquer que le groupe de travail des opérations du DNS (DNSOP) de l'IETF a deux propositions pour coordonner les informations de signature DNSSEC, mais se demande s'il ne serait pas préférable de créer un système général plutôt que de résoudre ce problème ponctuel. La coordination des adresses forward/reverse pourrait être une autre application.

Alors, de quoi a-t-on besoin ? Nous supposons que le modèle approprié est celui dans lequel l'ensemble des parties partageant le contrôle disposent d'un ensemble de fonctionnalités :

- un système pour initier une zone partagée, constitué par la zone elle-même ainsi que des règles et des journaux individuels pour que chacun des participants publie ses demandes et ses actions ;
- des vérifications techniques automatiques en cas de besoin pour la zone spécifique ;
- chaque type de demande est visible pour tous les autres participants qui peuvent approuver, désapprouver ou mettre en attente ;
- des règles définissant ce qui arrive à une demande
    - Un type de règle est un vote qui définit les conditions pour qu'une demande aboutisse. Elle peut inclure un délai pour que toutes les parties aient suffisamment de temps pour examiner la demande.
        - Pour les ccTLD, les règles du Sommet mondial sur la société de l'information (SMSI) préconisent 1 de N, de sorte que chaque domaine de premier niveau géographique (ccTLD) pourrait modifier unilatéralement ses propres données.
        - D'autres domaines pourraient appliquer la majorité simple
    - Les délais indiqués pourraient être importants pour que d'autres soient en mesure de signaler des problèmes opérationnels et que les demandeurs aient la possibilité de reconsidérer leur demande.
    - Des conditions différentes peuvent s'appliquer à des opérations différentes, comme la création versus l'édition, etc.

Par la suite, les participants pourraient créer un algorithme standard pour générer un état cohérent. Cela peut sembler fantaisiste, mais les algorithmes byzantins comme Bitcoin [Andreesen 2014] et Namecoin montrent que de tels systèmes sont possibles aujourd'hui.

(Notez que le panel ne propose pas des règles mais tout simplement un système distribué pour mettre en œuvre toutes les règles souhaitées par la communauté).

4.4.Opérations des opérateurs de registres/bureaux d'enregistrement

Certains membres du panel ont manifesté que les opérations de l'ICANN devraient fournir des garanties de niveau de service, mais le panel a considéré qu'il ne s'agissait pas d'une question qu'il pourrait faire avancer.

4.5. Quelles sont les données que l'ICANN devrait publier ?

4.5.1. Paramètres de l'ICANN

L'ICANN gère de nombreux ensembles de paramètres dans le cadre des fonctions de l'autorité chargée de la gestion de l'adressage sur Internet (IANA) ainsi que du nouveau processus TLD. C'est par exemple le cas des étiquettes réservées dans plusieurs langues. Tous ces paramètres doivent être mis à disposition en ligne, pourquoi pas dans le DNS et certainement de manière sécurisée, afin que toute la communauté Internet puisse les utiliser. D'autres propositions visent à l'utilisation du DNS comme un registre de blocs d'adresses, systèmes autonomes, etc.

4.5.2. Anniversaire des domaines, activités et bailliages

La réputation du DNS est un outil de sécurité important. Aujourd'hui, la date de création d'un nom de domaine est peut-être l'information la plus représentative de sa réputation. Le taux de mise à jour d'un domaine pour les noms de serveur et les adresses l'est aussi. Il est parfois important aussi de connaître quel bureau d'enregistrement a été utilisé pour créer et gérer un nom de domaine. Des domaines nouveaux, des activités de mise à jour trop importantes et certains bureaux d'enregistrement sont suspects. Il serait souhaitable que cette information soit disponible en temps réel, à grande échelle.

La question des informations de bailliage a également été abordée, mais elle a été reprise à l'IETF, en mars 2014 à Londres.

4.5.3. L'exemple LISP

Peu après sa création, le panel a été interrogé par rapport à la possibilité que l'ICANN soutienne un service super-racine pour le protocole de séparation de l'identificateur et du localisateur (LISP) [RFC 6830]. Comme Dino Farinacci et autres nous l'ont expliqué, l'ICANN exploiterait des serveurs LISP

comme un service expérimental pour renvoyer des requêtes aux serveurs LISP existants qui n'offrent pas actuellement une connectivité universelle. L'ICANN a alloué des ressources pour quatre serveurs, mais le projet n'a jamais pu démarrer en raison de certaines questions non résolues :

- quelle serait le champ d'application (durée, etc.) de l'expérience ? Quels en sont les critères de réussite ?
- quel serait le logiciel utilisé et qui le soutiendrait ? Deux solutions propriétaires étaient possibles.
- qui aurait le contrôle opérationnel et politique ?
- l'ICANN devrait-elle s'occuper du projet ou serait-il du ressort des registres Internet régionaux (RIR) ?
- la réponse serait-elle différente si les adresses IP n'étaient pas impliquées ?

Aucune mesure n'a été prise sur cette expérience.

Une partie du panel a estimé que « LISP n'est qu'un exemple d'une classe plus générique des technologies de tunnellisation du transport et qu'à ce titre ne présente aucune nouvelle tâche de gestion des identificateurs par rapport aux pratiques actuelles. Par conséquent, la nécessité pour l'ICANN d'y porter une attention et un soutien particuliers n'a pas été clairement établie ».

L'ICANN devrait prévoir que les questions techniques et politiques portant sur les nouveaux identificateurs vont réapparaître, et devrait planifier en conséquence.

4.6. Collisions

Beaucoup de membres du panel étaient familiarisés avec la question de la collision dans le DNS. Bien que de nombreuses discussions sur la question aient eu lieu, aucune nouvelle recommandation substantielle n'a été suggéré. Le panel trouve que le prototypage du système à échelle réelle décrit dans [ICANN 2013] est fortement recommandé.

5. Les bases du protocole DNS

Peut-on imaginer une révision fondamentale, une modernisation ou une renaissance du DNS ? Beaucoup, y compris certains membres du panel, croient que la base installée est trop résistante, ou que le processus est problématique[2], ou que repartir à zéro serait la meilleure solution.

[2] Les avis à cet égard varient. Certains disent que le processus IETF est bel et bien « fracturé » en groupes de travail spécifiques (spécialement dans le passé). D'autres considèrent que les API sont nécessaires et que l'IETF n'en fait pas, mais qui en fait ? D'autres pensent que la diversité des groupes de travail sur le DNS contribue à accélérer l'évolution et l'innovation mieux que ne le ferait une vision générale.

Chose étonnante, le panel croit à l'unanimité que l'effort de caractériser les problèmes et de chercher des solutions a valu la peine, ne serait-ce que pour laisser la question en suspens. Dans cette section, le panel présente quelques-unes des questions qui devraient faire l'objet d'une étude au cas où un effort plus large devrait être entrepris.

L'histoire de l'innovation dans le DNS a eu ses succès et ses échecs. Une des principales leçons à tirer est que la technologie n'est largement adoptée que si elle fournit un avantage particulier. Les administrateurs prennent soin de garder leurs zones connectées au DNS mondial et de mettre à jour leurs enregistrements A et MX ; autrement, ils ne recevraient pas de courrier ni de trafic Web. Mais sur les quelque 60 types d'enregistrements qui ont été définis, moins de 10 sont largement utilisés.

Les efforts pour créer des applications basées sur le DNS ont été confrontés à des difficultés similaires.

La première série de RFC relatifs au DNS a suggéré une méthode pour le routage du courrier vers des boîtes aux lettres spécifiques, mais celle-ci n'a jamais été appliquée. Un deuxième système, le MX RR, a résolu le problème des serveurs de messagerie redondants et de l'acheminement du courrier à travers les frontières organisationnelles (à l'heure actuelle, c'est la base de l'acheminement du courrier). Les bases de données anti-spam ont été largement adoptées sans normalisation. L'effort en vue d'établir des normes concurrentes pour l'authentification du courrier électronique a conduit à deux mises en œuvre utilisant des RR TXT et à un débat pour savoir si la normalisation des nouveaux types serait toujours utile.

L'initiative E.164 NUMber mapping (ENUM) pour normaliser le téléphone et d'autres routages de contenus multimédia à l'aide du DNS a également connu un succès très limité. Même si la technologie NAPTR (Pointeur d'autorité de nommage / Name Authority Pointer) est considérée comme une véritable innovation, les concepteurs de l'ENUM ont ignoré la nécessité d'acheminer des informations autres que le numéro de téléphone du destinataire, et les fabricants d'équipements ont préféré conserver la valeur de leurs systèmes propriétaires.

5.1. Principes généraux

Toute nouvelle conception doit :

- supprimer les limitations de taille - l'unité de transmission maximale (MTU) de 576 octets a contribué plus que tout autre facteur au retard du DNS ; le DNSSEC ne convient pas et malgré le mécanisme d'extension pour DNS (EDNS0), une grande partie du matériel et beaucoup de logiciels ne peuvent pas faire passer de grands paquets.
- préserver la connectivité pour tous les noms et données existants dans le DNS.
- essayer d'encourager des mises en œuvre cohérentes - si les différents responsables de la mise en œuvre ne respectent pas les spécifications, alors l'utilisateur est limité aux doublons existants.
- permettre l'expansion future.
- prévoir des encouragements pour son adoption.

5.2. Modèle de données

Les premiers RFC du DNS ont imaginé des espaces de noms parallèles pour différentes « classes » d'information et de nouveaux types de données construites à partir de composantes simples. La notion de classe n'a jamais été analysée. De nouveaux types de données ont été définis, mais plus récemment, beaucoup ont plaidé en faveur de l'utilisation d'enregistrements TXT génériques -destiné à des chaînes de texte arbitraires- avec un autre niveau d'étiquette pour transporter les données, à la place des enregistrements de type RR.

Le panel est d'avis que le DNS devrait définir ses propres types de RR et le format des métadonnées transportées par le DNS, ou bien formaliser les étiquettes enfant comme le dernier type de données et élargir la requête pour obtenir une correspondance plus flexible.

Enfin, nous devons explorer la piste des objets de données auto-signés, capables d'exister indépendamment du nom de domaine.

5.3. Distribution

La structure de zone des données et la mise en cache par l'enregistrement de ressource sont mises en œuvre avec des « améliorations » quelque peu inégales de la norme Temps à vivre (TTL) et la pré-extraction des informations arrivant à expiration. Il pourrait être utile d'envisager de nouvelles manières de grouper des données à l'aide de numéros de série, afin de pouvoir rafraîchir les groupes de données mises en cache sans que l'on ait à transférer réellement les données.

Le panel pense aussi que la sécurité pourrait être améliorée grâce à une réplication plus fréquente de zones (probablement plus petites), à l'aide des mécanismes existants de transfert de zone. Ces données n'ont pas besoin d'être sécurisées par le DNSSEC et peuvent donc améliorer la sécurité là où DNSSEC n'est pas mis en œuvre.

5.4. Interface de programmation d'applications (API)

L'API DNS existe sous deux formes : l'interface utilisateur et les noms au niveau de l'API. Dans les deux cas, nous pouvons bénéficier d'une syntaxe standard qui permet d'obtenir un nom de domaine pleinement qualifié (FQDN) explicite. La communauté des utilisateurs serait mieux servie par un ensemble cohérent de politiques de recherche à travers des interfaces UI, mais il n'est pas clair s'il est possible d'obtenir des fournisseurs pour ce faire.

L'API de programmation a connu plusieurs tentatives de révision qui ont pour la plupart échoué. Récemment, Paul Hoffman a fait une présentation sur un nouveau projet, avec des interfaces asynchrones et le soutien du DNSSEC. Ce travail a été par la suite communiqué à l'IETF de Londres, en mars 2014. Voir http://vpnc.org/getdns-api/

Mais indépendamment de l'API, il y a une question connexe à propos de l'endroit où la validation DNSSEC et le filtrage DNS (le cas échéant) doivent être effectués. Le panel a été unanime sur le fait que, techniquement, la résiliation du DNSSEC devrait être autorisée dans le système final (qui pourrait être une machine virtuelle, un ordinateur portable, un serveur dans l'environnement de l'utilisateur, etc., selon les préférences de l'utilisateur), même si cela pourrait être impossible à cause du routeur, du

pare-feu ou d'autres restrictions existantes. De même, dans la mesure où le filtrage DNS n'est pas forcément le choix de tout le monde, il devrait être sous le contrôle de l'utilisateur.

Rien de tout ce que nous venons de mentionner signifie que l'utilisateur ne puisse pas sous-traiter ces tâches à un fournisseur de services Internet (ISP) ou à un autre service.

Des contraintes politiques et juridiques peuvent stipuler le contraire.

5.5. Protocole de requête

Le protocole de requête DNS présente deux types de problèmes : premièrement, ceux relatifs au transport des requêtes / réponses d'un demandeur à un serveur, et deuxièmement, l'élargissement de la puissance de la requête.

La source des problèmes de transport UDP concerne la limitation traditionnelle de l'unité de transmission maximale à 576 octets (MTU). La correction initiale était d'avoir recours à la connexion TCP pour des transferts plus importants. La taille des données de la racine a probablement été le premier point sur lequel les limitations de l'unité de transmission ont eu un impact très répandu qui a abouti au nombre limité de 13 serveurs racine ; plus tard, l'ajout de signatures DNSSEC a sensiblement élargi les paquets de réponse. Le mécanisme d'extension pour DNS (EDNS0) a été conçu pour résoudre ce problème, entre autres, avec un certain succès. Mais il existe d'autres limitations telles que les différentes tailles des trames Ethernet ou les 1280 d'IPv6, etc., qui sont autant de contraintes pour l'UDP.

En outre, EDNS0 ne peut pas résoudre le problème des points d'accès, des routeurs, des pare-feux et d'autres matériels qui bloquent l'accès au port TCP 53, ou limitent la taille des paquets, ou même interceptent les requêtes DNS dans des proxys transparents, souvent au détriment du service. Des problèmes similaires peuvent être constatés dans des serveurs de noms cache qui ne supportent pas de grands paquets, tous les types de données DNS, EDNS0, etc. Certains problèmes peuvent être très subtils. Dans un exemple, les paquets DNSSEC passent normalement, mais pas pendant le déploiement des clés DNSSEC (un processus de maintenance normal) lorsque les paquets sont légèrement plus grands.

Les attaques par déni de service distribué (DDoS) du DNS sont un problème connexe, notamment les attaques par réflexion et par amplification. Dans ces cas, il est nécessaire de trouver un moyen de faire la différence entre le trafic légitime et le trafic d'attaque. La validation de l'adresse de la source [BCP 38] permettrait de résoudre une partie importante du problème, aussi bien pour le DNS que pour de nombreux autres protocoles. Le panel soutient cette possibilité[3], mais elle n'est pas largement déployée. Le lissage de débit et divers heuristiques peuvent aider, mais ne sont guère une solution définitive. Différents mécanismes légers d'authentification ont été et demeurent des candidats.

[3] Tous les membres du panel soutiennent l'idéal [BCP 38] et certains membres du panel considèrent que ce soutien devrait faire partie des recommandations clés du panel. Cependant, la plupart des membres du panel notent que son adoption a été très limitée depuis la publication du BCP en 2000.

Une théorie pour résoudre le problème du transport est de mettre tout le trafic DNS en https. La logique indique que tout le monde veut avoir un flux de trafic Web sécurisé, et cette voie en serait une garantie (certains disent que c'est la SEULE voie pour garantir le trafic). Le prix est celui de la connexion et des frais généraux associés. Les alternatives concernent certains nouveaux protocoles de transaction ou des moyens d'utiliser UDP ; les deux possibilités risquent de ne pas fonctionner dans certaines parties de la base installée. Dans les deux cas, il y a la question de savoir si les formats utilisés par les transactions DNS sont traditionnels ou nouveaux.

Indépendamment du transport, le protocole de requête DNS devrait être élargi pour permettre des requêtes plus flexibles. Celles-ci pourraient inclure une sorte de contrôle d'accès pour les nouvelles étiquettes au lieu de NSEC et NSEC3.

Les protocoles mondiaux de recherche tels que CCN ont tiré des apprentissages du DNS et incorporé toutes ces caractéristiques. Le problème pour ces nouveaux protocoles est plutôt celui de savoir comment motiver une mise à jour de l'infrastructure existante avec une certaine compatibilité en amont, plutôt que de donner lieu à une nouvelle avancée dans la science des protocoles.

6. Observations et recommandations

- L'utilisation du DNS dans l'infrastructure ne cessera pas d'évoluer. L'utilisation du DNS dans les interfaces utilisateur (UI) est confrontée à des alternatives basées sur la recherche, les interfaces mobiles, etc.
- L'ICANN devrait publier davantage de données signées DNSSEC pour des étiquettes réservées, etc.
- En coopération avec l'IETF et autres, mener une étude destinée à définir une vision architecturale du DNS en 2020.
- Concevoir et publier un prototype de racine ouverte.
- Concevoir un système de contrôle de zone partagé pour la racine.
- Mettre en place des exercices de collision afin d'en évaluer la facilité de mise en œuvre [ICANN 2013].

7. Références

[Andreesen 2014] Andreesen, « Why Bitcoin Matters », http://dealbook.nytimes.com/2014/01/21/why-bitcoin-matters

[BCP 38] Ferguson el al, "Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing", RFC 2827, mai 2000.

[DNS/TCP] https://lists.dns-oarc.net/mailman/listinfo/tcp-testing

[Fayazbakhsh 2013] Fayazbakhsh et al, « Less Pain, Most of the Gain: Incrementally Deployable ICN », Sigcomm 2013

[Ghodsi 2011] Ghodsi et al, « Naming in Content-Oriented Architecture », Sigcomm 2011

[Huston 2013] « DNS-over-TCP-only study ».

http://www.circleid.com/posts/20130820_a_question_of_dns_protocols/ et le fil suivant des opérations-dns

[ICANN 2013] « Guide pour l'identification et l'atténuation des collisions de noms pour les professionnels des TI », https://www.icann.org/en/about/staff/security/ssr/name-collision-mitigation-05dec13-en.pdf

[Kaminsky 2004] D. Kaminsky, « Tunneling Audio, Vidéo, et SSH sur DNS », BlackHat 2004

[Mérite] Articles sur les domaines et le DNS

http://www.afnic.fr/en/about-afnic/news/general-news/6391/show/the-internet-in-10-years-professionals-answer-the-afnic-survey.html

[Mockapetris 88] P. Mockapetris et K. Dunlap, « Le développement du système des noms de domaine », SIGCOMM 88

[Newyorker 2013]

http://www.newyorker.com/online/blogs/elements/2013/12/the-mission-to-decentralize-the-internet.html?goback=%2Egde_1430_member_5817512945197801473#%21

[RFC 881] J. Postel, « Le plan des noms de domaine et calendrier », novembre 1983.

[RFC 882] P. Mockapetris, « Noms de domaine - concepts et facilités », novembre 1983.

[RFC 883] P. Mockapetris, « Noms de domaine - mise en œuvre et spécification », novembre 1983.

[RFC 1034] P. Mockapetris, « Noms de domaine - concepts et facilités », novembre 1987.

[RFC 1035] P. Mockapetris, « Noms de domaine - mise en œuvre et spécification », novembre 1987.

[Spiegel 2014] http://www.spiegel.de/international/world/nsa-secret-toolbox-ant-unit-offers-spy-gadgets-for-every-need-a-941006.html

8. Glossaire

A Un type d'enregistrement DNS utilisé pour stocker une adresse IPv4

AAAA Un type d'enregistrement DNS utilisé pour stocker une adresse IPv6, appelé aussi « quad A »

AI Intelligence artificielle

API Interface de programmation d'applications

BCP Meilleure pratique actuelle -un sous-ensemble des RFC

CCN Réseau informatique basé sur les contenus

ccTLD Domaine de premier niveau géographique - TLD attribué à un pays en particulier, quelquefois opéré par une tierce partie.

DANE Authentification d'entités nommées basée sur le DNS

DDOS Déni de service distribué

DNS Système des noms de domaine - Système de nommage de l'Internet

Opérations DNSOP DNS - un groupe de travail de l'IETF consacré aux questions relatives aux opérations du DNS et autres

DNSSEC Extensions de sécurité du système des noms de domaine

DSL Ligne d'accès numérique

E.164 recommandation de l'UIT-T, intitulée *Le plan de numérotage des télécommunications publiques internationales* qui définit un plan de numérotage pour le réseau téléphonique public commuté (PSTN) et d'autres réseaux de données

EDNS0 Mécanisme d'extension pour le DNS [RFC 2671] – Norme d'extension pour étendre la taille et les champs des spécifications DNS d'origine

ENUM E.164 NUMber mapping - Système pour unifier le réseau téléphonique public commuté des télécommunications internationales avec l'adressage et les espaces de noms d'identification, par exemple pour acheminer un appel téléphonique

FEDEX Federal Express

FQDN Noms de domaine pleinement qualifiés

FTP Protocole de transfert de fichiers

gTLD Domaine générique de premier niveau - Un TLD qui ne correspond pas à un code géographique

HTTPS Protocole de transfert hypertexte sécurisé

IANA Autorité chargée de la gestion de l'adressage sur Internet

ICANN Société pour l'attribution des noms de domaines et des numéros sur Internet

ICN Réseau informatique basé sur les informations

IEEE Institut des ingénieurs électriques et électroniques

IETF Groupe de travail de génie Internet

IOT Internet des objets

IP Protocole Internet

IPSEC Protocole de sécurité IP

IPv4 Protocole Internet version 4

IPv6 Protocole Internet version 6

ITI Innovation technologique en matière d'identificateurs - panel de stratégie de l'ICANN

LISP Protocole de séparation de l'identificateur et du localisateur [RFC 6830]

MIB Base de gestion des informations

MTU Unité de transfert maximale - Taille maximale d'un paquet pouvant être transmis en une seule fois (sans fragmentation)

MX Mail Exchange – Les enregistrements Mail Exchange (MX) dirigent les e-mails d'un domaine vers les serveurs hébergeant les comptes utilisateur du domaine

NAPTR Pointeur d'autorité de nommage - Un type de données DNS couramment utilisé dans la téléphonie sur Internet

NDN réseaux informatiques fondés sur les objets nommés

P2P Pair à Pair

ICP Infrastructure des clés publiques

RFC Appels à commentaires – Mémos qui documentent les problèmes techniques et opérationnels de l'Internet

RIR Registre Internet Régional – Une des organisations qui gèrent l'attribution et l'enregistrement des ressources de numéros d'Internet dans une région du monde en particulier. Par exemple, ARIN, le registre américain des numéros d'Internet gère ceux du Canada, des États-Unis, et de nombreuses îles des Caraïbes et de l'Atlantique Nord.

Rsynch Protocole de synchronisation à distance – Ce protocole synchronise les fichiers et les répertoires tout en minimisant le transfert de données en utilisant le codage delta.

RR Enregistrement de ressource– l'unité atomique d'information dans le DNS

TSIG Signature de transaction

TTL Temps à vivre

TXT Le RR de type texte qui permet le stockage de champs de texte de format libre

UDP Protocole de datagramme utilisateur – Protocole de télécommunications sans connexion utilisé par l'Internet

UI Interface de l'utilisateur

URI Identificateur uniforme de ressources

URL Adresse universelle

WIFI Fidélité sans fil – les normes de réseau sans fil définies par la famille de normes IEEE 802.11

9. Contributions des membres du panel

Nous signalons que toutes les contributions sont reproduites textuellement, telles qu'elles ont été présentées par les participants.

9.1. Contribution de James Seng

Architecture technique

Le pirate qui habite en moi aime l'architecture de la décentralisation. On pourrait dire que la plupart des « problèmes politiques » existant à l'heure actuelle découlent du caractère centralisé du DNS par rapport à la racine.

Des technologies comme namecoins ou autres systèmes d'identification décentralisés me semblent complexes.

Or, il n'existe pas à l'heure actuelle de système d'identificateurs « décentralisé mais coordonné » qui soit largement utilisé. Que cela nous plaise ou non, le système DNS reste un des systèmes d'identification que nous avons. Comme on dit à l'IETF, ce sont les « codes en fonctionnement » qui l'emportent, ce qui ne veut pas dire qu'ils soient les mieux conçus.

Je ne crois pas en une racine multiple ou en une racine alternative. Comme je l'ai dit à Buenos Aires, je soutiens le RFC 2826. Multi-racine, racine alternative et toutes les propositions concernant ces questions ne font que déplacer le problème politique vers une autre couche, mais le problème politique fondamental n'est toujours pas résolu. Notez que j'ai dit problème politique parce que je ne pense pas du tout que la racine multiple puisse résoudre les problèmes techniques ; au contraire, cela augmente la complexité technique.

ICANN

Le DNS et la nature centralisée de la racine ont abouti à ce qu'une partie de l'opération -simple à l'origine- de la fonction IANA devienne l'énorme organisation qu'aujourd'hui on appelle l'ICANN.

J'ai participé à l'ICANN depuis sa première réunion en 1999 et j'ai assisté à presque toutes ses réunions. Au cours de ces années, j'ai trouvé qu'il y avait des questions que l'ICANN aurait pu aborder différemment, c'est à dire, notre position n'est pas toujours alignée.

Toutefois, l'ICANN est le « code en fonctionnement » de la coordination des identificateurs DNS. Il peut y avoir peut-être une meilleure conception, peut-être plus simple et élégante (beaucoup de membres de la communauté IETF souhaitent pouvoir revenir à l'époque de Jon Postel), mais c'est ce que nous avons

aujourd'hui : bien que perfectible, elle fonctionne. L'alternative proposée (UIT) que nous connaissons a d'autres problèmes qui sont peut-être pires.

Je soutiens donc l'ICANN car c'est tout simplement le meilleur système de travail dont nous disposons pour la coordination des identificateurs DNS et la racine.

Extension du DNS et de son système à d'autres secteurs

Par conséquent, je n'ai que peu d'intérêt à repenser le DNS ou à faire des propositions alternatives aux identificateurs de nommage. Éventuellement, il doit y avoir quelqu'un ou une organisation pour s'occuper de la coordination mais, le moment venu, nous serons confrontés aux mêmes problèmes politiques.

Je soutiens l'écosystème DNS (normes DNS, opération de la racine, l'ICANN, ...) que nous avons conçu à l'origine, un DNS qui évolue pour s'étendre à d'autres domaines (par exemple RFID), de manière à pouvoir incorporer une communauté plus large. Le travail que nous avons fait avec les IDN a consisté en quelque sorte à incorporer à l'écosystème du DNS un groupe d'utilisateurs de la communauté qui avait besoin d'utiliser sa propre langue maternelle, au lieu de les laisser construire leur propre système.

À ceux qui me disent que le déploiement des IDN aurait été beaucoup plus rapide en dehors de l'écosystème DNS (voir, par exemple, Mots-clés des langues autochtones), je réponds que les IDN sont meilleurs justement parce qu'ils font partie de l'écosystème DNS, où il y a des standards ouverts bien définis, des mises en œuvre ouvertes, des compagnies qui se basent sur la légitimité du DNS, et aussi la protection des titulaires d'IDN et des utilisateurs finaux.

Je n'en ai aucun doute et je soutiens la possibilité d'explorer des moyens d'étendre le DNS aux identificateurs même si à l'origine le système n'a pas été conçu pour cela. Les ingénieurs qui conçoivent les identificateurs sont souvent naïfs en ce qui concerne la politique qui accompagne les identificateurs, notamment si ceux-ci sont destinés à des utilisateurs finaux. Ils pourraient apprendre une chose ou deux de l'histoire des identificateurs du DNS et de l'ICANN.

Politique relative à la racine

La politique de l'ICANN et la façon dont certains considèrent son rôle dans la « gouvernance de l'Internet » sont liés au rôle de l'ICANN dans la coordination des serveurs racine.

Pour compliquer encore les choses, 11 des 13 serveurs racine sont basés aux États-Unis, suite à un accident historique, mais cela augmente néanmoins la perception que l'ICANN est sous le contrôle des États-Unis, en particulier après l'affaire Snowden.

Chaque fois que quelqu'un parle de tel ou tel pays qui devrait avoir un serveur racine, nous répondons par des arguments de type historique ou technique, en disant qu'il n'y a pas moyen d'étendre le nombre de serveurs racine au-delà de 13.

Je peux accepter l'argument historique.

Mais je ne peux pas accepter les arguments techniques. Ce sont plutôt des excuses, car je n'ai pas connaissance que l'IETF ait étudié sérieusement des moyens d'élargir le nombre de serveurs racine au-delà de 13. C'est pourquoi j'ai dit lors de la réunion de Buenos Aires que je peux penser à quelques solutions techniques qui pourraient suffire, comme un I-D. Nous ne pouvons pas laisser l'ICANN continuer à utiliser l'IETF ou les raisons techniques comme une excuse pour les problèmes politiques auxquels elle est confrontée. Nous devrions être en mesure de dire à l'ICANN, oui cela peut être fait, mais c'est à vous de décider de la politique à appliquer pour le faire.

Par ailleurs, et c'est plus important encore, le fonctionnement des serveurs racine n'est pas si central qu'on pourrait le croire.

Le fait d'avoir une racine ne signifie pas avoir immédiatement le contrôle de l'Internet. En fait, c'est aussi ennuyeux qu'une racine Anycast. Sauf que si l'opérateur de racine ne suit pas certaines des meilleures pratiques de fonctionnement du serveur racine (par exemple, RFC 2010 et RFC 2870), alors il peut causer beaucoup de tort à l'Internet.

La plupart des ingénieurs comprennent probablement ce que je viens de dire, mais ce n'est pas le cas de tous les membres d'ICANN.

Il y a donc des considérations dont il faut tenir compte lors de la sélection d'un opérateur de serveur racine dans la mesure où leur travail est clé pour la stabilité des identificateurs d'Internet, et cela est en grande partie basé sur la confiance. Mais la confiance, qu'on le veuille ou non, n'est pas un problème d'ingénierie.

-James Seng

http://chineseseoshifu.com/blog/dnspod-in-china.html

Pourquoi DNSPod est utile en Chine, en dépit de la façon dont il a « cassé » le DNS.

9.2.Résolution du DNS et comportement de l'application de la liste de recherche - Geoff Huston

aucun - ne garantit PAS la recherche DNS

jamais - recherche le nom de la base, mais ne s'applique pas à la liste de recherche

pré - s'applique à la liste de recherche, et s'il renvoie NXDOMAIN alors il recherche le nom de base

post - recherche le nom de base, et s'il renvoie NXDOMAIN il s'applique alors à la liste de

recherche

toujours - ne recherche PAS le nom de base - il s'applique seulement à la liste de recherche

Comportement de la bibliothèque du résolveur DNS du système d'exploitation de base

Système	**Absolu** *serveur.*	**Étiquette unique relative** *serveur*	**Multi-étiquette relative** *www.serveur*
MAC OSX 10.9	jamais	toujours	jamais
Windows XP	jamais	toujours	post
Windows Vista	jamais	toujours	jamais
Windows 7	jamais	toujours	jamais
Windows 8	jamais	toujours	jamais
FreeBSD 9.1	jamais	pré	post
Ubuntu 13.04	jamais	pré	post

Comportement du navigateur sur MAC et sur les plateformes Windows

MAC OSX 10.9

	serveur.	*serveur*	*www.serveur*
Chrome (31.0.1650.39 beta)	Jamais	toujours	pré
Opera (12.16)	Jamais	toujours	jamais
Firefox (25.0)	post*	toujours	post*
Safari (7.0 9537.71)	aucun**	aucun**	aucun**

* Ajouter le préfixe « www. », puis essayer de mettre un préfixe à « www. » en ajoutant également la liste de recherche.

** Safari semble reconnaître les TLD et n'effectue pas les recherches DNS lorsque le nom n'est pas un TLD.

Windows 8.1

	serveur.	*serveur*	*www.serveur*
Explorer (11.0.900.16384)	aucune	aucune	jamais
Firefox (25.0)	jamais*	toujours	jamais
Opera (17.0)	aucune	aucune	aucun**
Safari (5.1.7 7534.57.2)	jamais*	toujours***	jamais

* ajouté à préfixe de « www »

** OPERA reconnaît les tld délégués et ne demande que quand la dernière étiquette est un TLD

*** ajouté un préfixe de « www » et un suffixe de « .com »

9.3. Observations en matière de cohérence et d'écart - Contribution de Geoff Huston

Si l'on remonte aux origines du système de noms de domaine, on retrouve des « fichier hosts », une première tentative d'introduire des noms liés à l'activité humaine dans le contexte des réseaux informatiques. L'ARPANET utilisait un modèle de nommage des nœuds du réseau où chaque nœud connecté avait un fichier de configuration local, le fichier « hosts », qui contenait les noms de tous les autres nœuds du réseau ARPANET et les adresses de protocole de chaque nœud. Aucune uniformité n'était exigée pour les multiples instances de ce fichier HOSTS sur l'ensemble des nœuds ARPANET connectés, et il n'y avait pas non plus, à l'époque, une méthode pour distribuer une copie du fichier hosts à travers le réseau. L'utilité de ce fichier hosts était de fournir des noms conviviaux au lieu des noms barbares des adresses de protocole. Les utilisateurs étaient en mesure d'identifier les nœuds du réseau par leur nom symbolique, qui était ensuite traduit en une adresse binaire spécifique au protocole grâce à une recherche dans le fichier hosts. L'évolution d'ARPANET s'est accompagnée d'une augmentation de la taille et du taux de mise à jour du fichier hosts, ainsi que des frais associés au maintien de la précision des fichiers hosts locaux. Le format du fichier hosts a été normalisé (RFC952) et un service de fichier hosts central capable de réunir de nombreuses copies locales du fichier hosts a été défini (RFC953).

Cela fut ensuite remplacé par le système des noms de domaine (DNS), décrit pour la première fois en 1983, dans le RFC 882 et le RFC 883. Le mécanisme de traduction d'un nom – spécifié comme une chaîne

conviviale pour l'homme– en une adresse de service spécifique à un protocole a été maintenu dans la transition du fichier hosts au DNS.

Cet espace d'identification possède un certain nombre de propriétés, dont le fait que tout en étant adapté au discours humain, l'espace de noms DNS possède une structure formelle qui permet son utilisation déterministe par des applications informatiques. L'espace de noms DNS est un espace structuré de manière hiérarchique qui permet la recherche de correspondances exactes ainsi qu'un cadre de gestion distribuée des noms. Si les collisions d'étiquettes sont évitées dans une zone individuelle de la hiérarchie des noms du DNS, les collisions de noms peuvent être évitées dans l'espace global de noms DNS, facilitant ainsi la gestion de la nature unique des noms dans le cadre du DNS. Le DNS est flexible en termes de cartographie et peut être utilisé pour mettre en correspondance un espace de noms structuré avec toute autre forme de ressources nommées que notre service désigne. Le DNS est destiné à être cohérent en ce sens que toute requête concernant un nom figurant dans le DNS devrait donner lieu à la même réponse, indépendamment de la localisation de celui qui envoie la requête et du moment où la requête est envoyée. Cette cohérence référentielle permet qu'un nom soit communiqué d'une partie à l'autre sans que la référence à la localisation du service soit modifiée. Le DNS n'est pas destiné à se substituer à un système de répertoire ou à un système de recherche. S'il existe une correspondance exacte entre le nom recherché et un nom contenu dans le DNS, la requête DNS renverra la valeur cartographiée comme résultat de la requête ; sinon, la requête aboutira à un échec de correspondance.

Ce modèle d'identification utilisé dans l'espace de noms DNS pour assurer l'interface entre l'homme et le réseau a subi par la suite un certain nombre de changements, notamment pour répondre à l’utilisation des identificateurs dans le discours humain. Nous avons tendance à utiliser les identificateurs de façon moins précise, avec des éléments de contexte associés à des langues et des écritures locales. Au fil du temps, le rôle du DNS en tant qu'interface humaine avec les ressources et les services du réseau a été réétudié dans le cadre d'initiatives qui cherchent à développer des interfaces capables d'interagir de façon plus « naturelle » avec les êtres humains.

Le RFC1034 a proposé l'utilisation d'une forme de raccourci dans la spécification de noms DNS, où les noms qui ne se terminent pas par '.' étaient qualifiés de « noms relatifs » et, comme indiqué dans le RFC1034, les « noms relatifs apparaissent surtout au niveau de l'interface utilisateur, où leur interprétation varie d'une implémentation à l'autre ». Typiquement, une telle interprétation locale comprend l'application d'une liste de recherche locale de suffixes d'étiquette, ce qui permet à l'utilisateur de spécifier la partie initiale d'un nom de domaine, et de confier à l'application locale ou aux routines logicielles de résolution de noms le soin d'ajouter un suffixe défini localement pour former un nom DNS complet.

Cette forme d'occlusion sélective de l'espace d'identificateurs du DNS par l'utilisation de suffixes de noms a été poussée un peu plus loin dans l'interface utilisateur proposée par les navigateurs Web, où il est fréquent que l'identifiant DNS d'une URL se voit appliquer une transformation du nom qui suit la chaîne « www », auquel on ajoute un suffixe défini localement (typiquement « .com »). De cette

manière, l'identificateur que l'utilisateur a spécifié et le nom de l'identificateur utilisé dans la requête DNS ultérieure restent liés, mais ne sont pas forcément les mêmes.

Cette utilisation des transformations de noms au niveau local a été appliquée à la manière dont les identificateurs formés à partir de scripts de langues autres que US ASCII étaient cartographiés dans les DNS (IDN : RFC5891). Il y a là un processus explicitement défini où l'identificateur saisi par l'utilisateur est transformé en une chaîne d'étiquette codée qui constitue la requête DNS. Dans ce cas, la transformation est définie avec précision, de sorte que plusieurs mises en œuvre de la norme IDN puissent donner lieu à une mise en correspondance cohérente entre un identificateur dans un script donné et une forme de nom DNS codée.

Une autre évolution du raffinement du modèle basé sur l'interaction humaine concerne l'unification des termes recherchés et des URL saisis dans les navigateurs. Dans ce cas, si l'utilisateur n'a pas utilisé la spécification complète d'une URL dans le navigateur, le navigateur va tenter de la compléter.

9.4. Problèmes liés aux technologies actuelles en matière d'identificateurs

1. Résilience de la zone racine

Aujourd'hui, le système DNS dépend beaucoup de la disponibilité, de la capacité et de l'accessibilité des serveurs racine. Si une entreprise, un FSI, un pays ou un utilisateur gardaient leur propre copie (ou leurs propres copies) de la zone racine et l'utilisaient pour résoudre les noms de domaines au lieu de se diriger toujours vers les serveurs racine « réels », l'entreprise, le FSI, le pays ou l'utilisateur seraient protégés de toute attaque adressée aux serveurs racine et seraient en mesure de continuer à fonctionner normalement lorsqu'ils seraient déconnectés des serveurs racine réels, ou lorsque ceux-ci seraient inaccessibles, surchargés ou compromis.

2. Utilisation frauduleuse des adresses IP

Les paquets IP avec des adresses source falsifiées comptent parmi les outils les plus importants dont disposent aujourd'hui les malfaiteurs pour empêcher leurs cibles d'utiliser l'Internet. En envoyant des paquets qui semblent venir de la cible et en faisant cela à partir d'un grand nombre de machines, l'attaquant provoque un grand trafic de « réponse » qui va colmater ou surcharger les liens du réseau qui retournent vers la cible.

3. Fast flux des correspondances noms-adresses dans le DNS

À l'heure actuelle, l'utilisation du système DNS est souvent détournée par des malfaiteurs qui s'en servent pour empêcher les autorités de retrouver la trace de leurs activités illégales et y mettre fin. Un opérateur de « réseau zombie » peut se servir d'un groupe de machines piratées (réseau zombie) pour s'adonner à plusieurs types d'activités illicites dont le spam, le lancement d'attaques DDOS et l'infection de différents types de machines à l'aide de logiciels malveillants. En changeant rapidement la correspondance noms-adresses (name-to-address mapping) dans le DNS, les opérateurs de réseaux

zombies peuvent vite faire basculer leurs activités illégales d'un groupe d'ordinateurs piratés à un autre afin d'empêcher les autorités de suivre la trace de leurs activités et y mettre fin.

Nous recommandons que l'ICANN travaille avec d'autres membres de la communauté Internet

(1) pour améliorer la résilience de la zone racine ;

(2) pour lutter contre l'utilisation frauduleuse des adresses IP ;

(3) pour aborder le problème du fast flux des correspondances noms-adresses dans le DNS.

9.5. Anycast universelle pour la zone racine - Paul Vixie

Aperçu

Nous proposons que l'IANA produise plusieurs formes supplémentaires de la zone racine du DNS, pour permettre la recherche anycast universelle et la recherche opérationnelle. « Anycast universelle » dans ce contexte fait référence à une zone racine dont les enregistrements NS du sommet listent seulement deux serveurs de noms, dont les adresses « bien connues » (comme indiqué par les enregistrements A et AAAA) peuvent être hébergées par n'importe qui. « La recherche opérationnelle » dans ce contexte comprend des essais publics à large échelle des serveurs de noms racine utilisant uniquement IPv6 et des essais publics à grande échelle des effets de la collision de noms avec les « nouveaux gTLD ». Cette approche traite le service de nom racine comme un utilitaire non géré plutôt que comme un utilitaire géré.

Contexte

Le déploiement d'anycast universelle pour la zone racine ne pouvait pas se faire de manière sûre et responsable avant le développement de DNSSEC, car sans DNSSEC, tout serveur donnant une réponse pouvait être configuré avec des données racine DNS arbitraires, y compris les nouveaux TLD ou les TLD existants redélégués. Avec DNSSEC, il est maintenant possible pour les opérateurs des serveurs de noms récursifs de configurer une validation DNSSEC de manière à ce que toute information gTLD venant d'un serveur de noms racine avec anycast universelle soit approuvée par l'IANA, tel qu'indiqué dans les signatures DNSSEC réalisées avec la clé de signature de zone racine de l'IANA (ZSK).

Les critiques au système de serveurs de noms racine actuel et historique visent sa faible résistance à une attaque DDoS et le fait que même avec l'anycasting actuel mis en place à grande échelle par tous les opérateurs des serveurs de noms racine, il n'y a encore que quelques centaines de serveurs de noms dans le monde qui peuvent répondre avec autorité pour la zone racine du DNS. Le fait que l'accessibilité du système de serveurs de noms racine soit nécessaire même pour la communication purement locale nous préoccupe aussi, car c'est le seul moyen pour les clients non locaux de découvrir les services

locaux. Dans un système mondial et distribué comme l'Internet, les services essentiels doivent être extrêmement bien distribués.

Détails

Il existe plusieurs variantes utiles qui peuvent être construites. Tout d'abord, l'anycast universelle de base permettra à tout opérateur de serveur de noms de capturer le trafic dirigé vers le système de serveurs de noms racine et d'y répondre localement. L'IANA génère et signe numériquement (à l'aide de DNSSEC) une version supplémentaire de la zone racine qui contient un ensemble différent d'enregistrements NS à son sommet. Ces enregistrements NS désigneront les serveurs de noms dont les adresses ne sont pas attribuées à un opérateur particulier de serveur de nom racine (RNSO) mais sont plutôt détenues en fiducie par l'IANA pour une utilisation par une ou par toutes les parties intéressées. L'IANA demande aux registres Internet régionaux (RIR) (tels qu'ARIN ou APNIC) des micro-attributions d'infrastructure, comme par exemple plusieurs préfixes de IPv4 24 bits et plusieurs préfixes IPv6 48 bits, pour les utiliser dans l'anycasting universelle de la zone racine.

Une seconde variante de la zone racine actuelle permettrait de fournir une anycast universelle comme ci-dessus, mais désignerait des serveurs de noms n'ayant que la connectivité IPv6 (indiquée par la présence d'enregistrements AAAA) et pas de connectivité IPv4 (comme indiqué par l'absence d'enregistrements A). Cette variation faciliterait la recherche opérationnelle dans un réseau constitué uniquement d'adresses IPv6.

Une troisième variante de la zone racine actuelle permettrait de fournir une anycast universelle comme ci-dessus, mais inclurait des délégations pour tous les nouveaux gTLD bien connus, y compris ceux qui autrement ne seraient pas prêts à la délégation (tels que .CORP et .HOME). Ces nouveaux gTLD seraient délégués à un serveur de noms opéré par l'IANA elle-même, à des fins d'évaluation. Chaque nouveau gTLD se verra attribuer des enregistrements A et AAAA génériques (ou Joker), dont les adresses communiqueront avec des serveurs Web exploités par l'IANA à des fins d'évaluation.

Impact

Étant donné la nature hiérarchique du routage de l'Internet, les blocs d'adresses anycast peuvent être annoncés à plusieurs niveaux. Une machine virtuelle (VM) fonctionnant dans un ordinateur portable peut avoir son propre processus de serveur de noms associé aux bonnes adresses connues, auquel cas aucune requête de service de nom racine ne quittera cette VM. L'ordinateur portable lui-même peut également capturer le trafic sortant destiné à ces adresses bien connues, qui serait utilisé par d'autres VM ou d'autres processus en cours d'exécution sur cet ordinateur portable. Le routeur sans fil en amont de cet ordinateur portable peut avoir des serveurs à l'écoute de ces adresses, auquel cas aucune requête du serveur de noms racine ne quittera ce LAN sans fil. Le FSI pourrait faire fonctionner des serveurs qui écoutent ces adresses bien connues, pour servir tous les clients qui n'exploitent pas leurs propres serveurs. Enfin, l'Internet mondial devrait avoir de nombreux opérateurs qui annoncent les routes à ces blocs d'adresses bien connus, parmi lesquels se trouveraient les douze opérateurs de serveurs de noms racine existants.

L'impact positif de cela serait une plus grande résilience potentielle et la réduction de la latence de service de noms racine. L'impact négatif serait la réduction des capacités de diagnostic et une vulnérabilité accrue aux « empoisonnement de route » ou aux « détournements » du trafic du service de noms racine. Il est en tout cas essentiel que la validation DNSSEC devienne habituelle afin de réduire les conséquences de ce type de piratage. Nous voulons que le résultat pour un attaquant soit « la perte du service de noms racine pour la victime » plutôt que « la victime voit un espace de noms DNS différent ».

Exemples

Les exemples suivants montrent l'ensemble d'enregistrements NS du sommet pour chaque variante de la zone racine, y compris l'enregistrement glue. Ces données seraient incluses dans une variante de zone racine avant la signature DNSSEC et publiées comme fichier « root hint ». Les données présentées pour iana-servers.net seraient également présentes dans la zone réelle iana-servers.net. Pour ces exemples, il faudrait quatre micro-attributions IPv4 et six micro-attributions IPv6.

Variante 1 : anycast universelle

```
. IN NS anycast-1.iana-servers.net.
. IN NS anycast-2.iana-servers.net.
$ORIGIN iana-servers.net.
anycast-1 IN AAAA 2001:?:1::1
anycast-1 IN A ?.?.1.1
anycast-2 IN AAAA 2001:?:2::2
anycast-2 IN A ?.?.2.2
```

Variante 2 : anycast universelle uniquement IPv6

```
. IN NS v6only-1.iana-servers.net.
. IN NS v6only-2.iana-servers.net.
$ORIGIN iana-servers.net.
v6only-1 IN AAAA 2001:?:3::1
v6only-2 IN AAAA 2001:?:4::2
```

Variante 3 : anycast étude de collision des gTLD

```
. IN NS gtldstudy-1.iana-servers.net.
. IN NS gtldstudy-2.iana-servers.net.
$ORIGIN iana-servers.net.
gtldstudy-1 IN AAAA 2001:?:5::1
gtldstudy-1 IN A ?.?.5.1
```