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

Panel sur l'innovation technologique en matière d'identificateurs – Rapport préliminaire

Le 21 février 2014

Table des matières

1. Introduction

Le panel sur l'innovation technologique en matière d'identificateurs (ITI) a été chargé par la Société pour l'attribution des noms de domaine et des numéros sur Internet (ICANN) d'atteindre les objectifs suivants :

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

2. développer des recommandations de meilleures pratiques et des systèmes de référence

3. fournir des orientations technologiques pour les opérations de l'ICANN, ses fonctions techniques, politiques et de sécurité

4. s'engager avec la communauté de l'ICANN et avec le public sur les questions touchant à la technologie

Le panel a été sélectionné en septembre et octobre 2013, et Paul Mockapetris a été élu président. Tous les membres travaillent à titre personnel, et leur affiliation est incluse seulement à des fins d'identification :

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

Des réunions en tête à tête ont eu lieu à la réunion de l'IETF de Vancouver (novembre 2013), à la réunion de l'ICANN de 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 électroniques par e-mail, et autres ont complété ces échanges. Le rapport sera disponible pour commentaires du public en février 2014, et il sera terminé après la réunion de l'IETF qui se tiendra en mars à Londres.

Le président tient à remercier le panel pour sa collaboration et les idées apportées ainsi que l'ICANN pour avoir donné son soutien au panel. Il remercie également Elise Gerich et Alice Jansen de l'ICANN qui ont contribué avec leurs idées et leur soutien à tous les travaux du panel.

2. Panel de stratégie

Le nom du panel n'a pas été choisi par hasard. Le champ d'application a été étendu au-delà du DNS en reconnaissance 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 universels (URI)
- la base de gestion des informations (MIB)
- la base de données des zones horaires

Cependant, parallèlement à cette expansion, le temps de travail du panel a été réduit de la période initiale d'un an à six mois environ. En conséquence, tout est plus ciblé sur le DNS.

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 de l'architecture du processeur)
- identifier les besoins « brûlants »
- éviter de se concentrer sur les « domaines bien traités » (par exemple le déploiement du DNSSEC, les stratégies existantes pour 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 idées proches des 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 serait plus naturellement appropriée pour l'IETF ou ailleurs. Certaines de ces idées soulèvent des questions de politique que nous n'avons pas abordées, dont nous avons tout simplement signalé l'existence.

Enfin, compte tenu de l'énorme activité dans l'espace des identificateurs, le panel a tout simplement échantillonné l'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 sont une question sensible pour la communauté Internet. À court terme, les nouveaux domaines de premier niveau (TLD) seront en ligne. Votre compte Facebook cherche à devenir votre identification unique d'ouverture de session pour l'Internet - comme votre compte Google. À long terme, la communauté des chercheurs envisage beaucoup de projets différents, y compris *Content Centric Networking* (CCN), *Information Centric Networking* (ICN), *Named Data Networking* (NDN),et bien d'autres variantes. Bien qu'ils ne puissent pas se mettre d'accord sur un nom pour le champ, ils sont tous d'accord sur le fait que le contenu doit être identifié par son nom, et non pas par son emplacement, et que la mise en cache serait opportuniste. D'autres propositions ont insisté pour dire que les noms plats sont la voie de l'avenir, et que l'auto-certification des noms devrait être la base de tout nouveau système.

Les identificateurs sont au centre de tout réseau en termes de composantes d'identification unique du réseau par rapport à toutes les autres composantes du réseau. En outre, les réseaux modernes ne sont pas constitués comme un seul domaine homogène mais sont construits comme un amalgame d'un certain nombre de technologies et il existe la nécessité de faire une cartographie des différents domaines d'identité. Cette fonction de cartographie est effectuée de différentes manières. Dans le contexte de l'Internet, l'un des domaines les plus visibles d'identité est le domaine du nom de domaine, qui est un espace de noms structuré hiérarchiquement. La fonction de cartographie est associée à cet espace de noms et permet de faire la cartographie des noms domaines et d'autres d'identités (comme les adresses IP, par exemple). Lorsque l'on regarde une feuille de route pour les identificateurs il faut que l'on soit au courant de la distinction entre le domaine de l'identificateur et la fonction de cartographie, et regarder la feuille de route pour chacun d'eux.

Dans l'Internet actuel, le panel a identifié plusieurs facteurs qui ont tendance à étendre l'utilisation du DNS, ainsi que plusieurs qui vont le contracter. Tous ces aspects ne sont pas techniques, et la lutte semblait plus darwinienne que basée sur l'élégance ou une autre vertu.

Facteurs d'expansion actuels

- Le DNS bénéficie d'un avantage hérité dans la mesure où il existe dans chaque dispositif qui utilise l'Internet. La simple croissance dans la base existante va élargir son utilisation. Par exemple, une application qui veut passer à travers les pare-feux et être mise en cache à travers l'Internet trouve le DNS comme une base existante.
- Les nouveaux TLD vont tenter de monétariser leurs marques. Bien qu'il règne un certain scepticisme au sein de la communauté technique, plus d'un millier de nouvelles marques vont lutter pour prospérer, et il semble qu'il y aura des innovations et de nombreuses surprises.
- Les nouvelles fonctionnalités émergentes, telles que les capacités de sécurité des extensions de sécurité du système des noms de domaine (DDNSSEC) ou le protocole DANE (*DNS-based Authentication of Named Entities*) peuvent motiver une utilisation supplémentaire.

- De nouvelles données dans le DNS pourraient étendre son utilisation, notamment lorsqu'il est combiné avec DNSSEC pour garantir l'authenticité. Un membre du panel a recommandé de publier l'« anniversaire » et l'« activité » des domaines comme l'information de base sur la réputation. D'autres proposent d'utiliser le DNS comme un registre de blocs d'adresses, etc. L'ICANN a restreint l'utilisation de certaines étiquettes dans les noms de domaine, et un registre de temps réel pourrait être approprié, notamment lorsque les spécifications sont fournies en plusieurs alphabets.

Facteurs de contraction actuels

- Le DNS est la norme héritée, mais c'est aussi un handicap dans cette logique du DNS intégré dans les points d'accès WIFI, les modems câblés et la ligne d'accès numérique (DSL), les pare-feux, les routeurs, et le logiciel de base de l'Internet qui limitent souvent la portée de l'utilisation et l'innovation. Les implémentations sont souvent moins complètes, actuelles ou conformes aux normes. Ces questions ont entravé la mise en œuvre du DNSSEC et ont rendu problématique la mise en œuvre de nouveaux types ou fonctions du DNS. Cela a amené à concevoir des pratiques telles que la limitation de son utilisation aux enregistrements d'adresses et de texte (TXT). Cette ossification n'affecte pas seulement le DNS.
- Il existe un intérêt commercial concernant le contrôle (« la possession ») de la fenêtre de recherche et / ou de l'espace de l'identificateur. L'intérêt porte ici sur le fait de voir l'intention de l'utilisateur en liberté et de le dissimuler de l'Internet ouvert. Nous avons identifié une tendance vers les dispositifs codés en dur pour un service de DNS spécifique, ainsi que les 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 est l'appareil 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. À titre d'exemple, Geoff Huston (voir contribution) a observé que la recherche déclenchée par « Geoff.Huston » dans plusieurs navigateurs n'avait pratiquement AUCUNE cohérence entre les fournisseurs. Ce manque de cohérence peut être tolérable dans une recherche par navigateur où l'utilisateur devrait vérifier les résultats, mais peut être dangereux dans les fichiers de configuration des systèmes — une des préoccupations est la récidive de collisions.

Le panel a évalué que tandis que l'utilisation du DNS peut disparaître de l'interface utilisateur, elle peut rester un outil d'infrastructure. Une analogie est que le DNS n'est pas comparable au livre de papier face à l'essor du livre électronique, mais plutôt un ensemble d'instructions de l'ordinateur qui est accessible par le biais de langages de niveau plus élevés.

Les opinions sont divergentes quant à savoir s'il était possible ou souhaitable de rechercher la renaissance ou la restructuration du DNS. La technologie est décrite dans la section « fondements du

DNS » de ce rapport. Il existe une question politique, à 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, fondée sur les différents points de vue de l'unité constitutive de l'ICANN, de l'IETF (où le travail serait probablement fait) et d'autres parties de l'Internet ?

Le long terme

Un ensemble d'idées sur le long terme est 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. Le modèle pour les requêtes de routage est parfois exprimé en utilisant simplement une hiérarchie de nom pour que les préfixes plus longs correspondent aux décisions de routage, ce que les sceptiques trouvent non échelonnable. En tout cas le logiciel, le matériel, et plusieurs bancs d'essai de réseau sont mis en œuvre. Les applications les plus évidentes sont la distribution de contenu, mais les défenseurs affirment que le modèle est bon pour le contrôle de processus, les réseaux automobiles, etc.

D'une certaine façon, le DNS a été la première des alternatives à l'ICN (Information Centric Networking), comme les approches les plus actuelles [Fayazbakhsh 2013] qui essaient de préserver seulement les parties les plus importantes du modèle ICN. L'importance ici est dans l'œil de celui qui regarde.

Le DNS extrait les données par nom. Il ne cherche pas à acheminer par nom, au lieu de cela il utilise la couche d'adressage de l'Internet. Ce système corrige ce que certains considèrent comme le problème central d'évolutivité pour l'ICN. Le DNS a été notoirement connu comme un véhicule pour le tunnel vidéo [Kaminsky 2004] et pour les tunnels illicites d'accès à travers les requêtes DNS qui sont effectuées avant l'authentification par certains points d'accès WIFI. (La recherche sur Google « tunnel DNS » renvoie 1 620 000 résultats environ.)

L'ICN a le plus long préfixe de correspondance et des sélecteurs qui permettent le transport de média, des installations qui ont été prévues dans la section de recherche 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.

En conclusion, on pourrait imaginer un système de réseau fondé sur des objets nommés (NDN) pour remplacer le DNS, commençant comme un sur-ensemble des installations de DNS dans une transition qui pourrait durer des années, voire des décennies. Toute tentative visant à améliorer l'architecture du DNS doit emprunter librement dans le NDN.

Le modèle ICN est loin d'être le seul modèle pour l'avenir, il est seulement l'un des plus développés. Nous croyons qu'il est toujours utile d'essayer, de résumer les principes de base et ensuite étudier la

composition. [Ghodsi2011] est un bon exemple de la façon dont il identifie la trinité du nom, l'ID réel du monde, et de l'infrastructure à clés publiques ICP.

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'ICP qui existe représente une ressource pour la surveillance à grande échelle et en conséquence un problème pour la confidentialité. Un mélange d'objets d'auto-certification, et une ICP de type opt-in ou encore des ICP parallèles et des systèmes pair à pair (P2P) pourrait être la réponse.

4. Questions opérationnelles

Plusieurs questions découlent des opérations quotidiennes de l'ICANN. Elles tournent essentiellement autour de la racine.

4.1.Durcissement de la racine

Compte tenu de l'importance cruciale de l'infrastructure de la racine, il y a eu plusieurs suggestions externes pour que le panel analyse les technologies informatiques fiables. Le panel a pensé qu'il pourrait y avoir du mérite pour ce type de technologie dans les systèmes utilisés pour modifier et signer la racine, mais il a résolu que le fait d'améliorer la distribution des données signées sur du matériel standard était une meilleure priorité pour le panel. Les révélations de Snowden soulèvent des préoccupations sur la sécurité du matériel qui peut ne pas avoir été prise en compte dans la conception des systèmes actuels, tels que les infections du BIOS, les logiciels espions du disque dur, etc. [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 ultime dans le cadre d'une zone, voyage avec cette zone dans un ou plusieurs transferts de zone, et arrive finalement à sa destination finale via 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 distribué à tous les serveurs racine via les transferts de zone. Sur le plan conceptuel, cette distribution, comme 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 de zone différentiel qui envoie les modifications d'une version précédente plutôt que toute la zone. Des copies peuvent être soit poussées par notification DNS ou par une stratégie de sondage qui

examine les modifications. La sécurité pour les transferts de zone peut se faire via signature de transaction du DNS (TSIG) et / ou par un certain nombre de protocoles de transport, par exemple, le protocole de sécurité IP (IPsec), le protocole de transfert hypertexte sécurisé (HTTPS), etc. Il y a des centaines de cas de serveurs racines 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 : en premier lieu, l'adresse IP de destination dans la requête identifie un ensemble de serveurs racine qui partagent une adresse anycast commune, et en deuxième lieu, le système de routage décide quel serveur dans l'ensemble anycast obtiendra effectivement la requête. Ce programme est le résultat d'une évolution qui a commencé avec 3 serveurs racine avec des adresses unicast ; par la suite il a été élargi à 13 organisations de serveur racine avec des clusters de charge partagée, et finalement le régime actuel (avec de nombreuses petites étapes entre les deux). Pour le dire plus simplement, cela signifie que les « 13 serveurs racine » sont vraiment « 13 organisations de serveurs racine » qui finalement délivrent 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 relâcher la limitation de la taille des paquets du protocole de datagramme utilisateur DNS (UDP). Il existe aussi d'autres problèmes de taille liés à l'ajout d'adresses IPv6. Le DNSSEC peut éventuellement assurer la sécurité du chemin du serveur racine vers l'utilisateur.

Au fil des ans, les serveurs racines 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 de toutes les adresses anycast des 13 organisations de serveurs racine différentes. La perturbation d'un sous-ensemble provoquera le ralentissement des performances tandis que le demandeur apprend quels sont les serveurs racine à éviter. La perturbation peut mettre hors service le serveur ou le chemin de réseau vers le serveur, en général avec une surcharge. Ainsi, par exemple, dans une attaque de ce genre, les utilisateurs de Californie pensaient que le serveur racine à Stockholm était en panne, alors qu'à Stockholm les utilisateurs pensaient le contraire. La réponse des organisations de serveurs racine à une menace récente de l'organisation pirate *anonyme* était de déployer davantage de bande passante, serveurs et fanfare.

Bien entendu, l'attaque n'a pas besoin d'être dirigée contre la constellation du serveur racine, elle peut être dirigée contre la/les connexion/s de l'utilisateur à l'Internet. Bien que plus limitée par rapport aux dommages, le rapport des forces entre une attaque des réseaux zombies et une seule entreprise est généralement beaucoup plus en faveur de l'attaquant, même pour les grandes 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 de serveur racine dans l'organisation de serveur racine de l'ICANN. C'est aussi une bonne idée pour une

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

entreprise d'être internement auto suffisante à l'égard du DNS, et de ne pas être menacée par le manque d'accès à des serveurs externes, ou par des actions réalisées par un opérateur de registre, bureau d'enregistrement, opérateurs de serveurs racine, etc., que ce soit par accident ou intentionnellement.

Compte tenu de DNSSEC, nous avons un moyen de distribuer une zone qui peut être vérifiée à l'aide de signatures numériques intégrées. Nous pensons que le principe peut être étendu, par exemple en protégeant la délégation et les données de type glue. Il peut également être possible d'éliminer ou de réduire l'organisation du serveur racine et des données d'adresse. Un procédé décrit en détail dans la contribution de Paul Vixie, est inclus dans la section Contributions de ce rapport.

Il existe aussi des aspects politiques importants. Il existe 13 organisations de serveurs racine, et plusieurs pays sentent qu'ils ont été oubliés, même s'ils sont en mesure d'avoir autant d'instances de serveurs racine de l'ICANN qu'ils le décident dans leur pays. (Sans compter que plusieurs autres organisations de serveurs racine sont prêtes à avoir leurs constellations anycast élargies). Alors, laissons le problème de côté.

Il convient de noter qu'il n'existe aucune nécessité technique de remplacer le système de serveur racine existant pour ceux qui le préfèrent ; nous allons simplement faire en sorte que la réplication pour la racine soit plus facile, et donner un exemple à d'autres zones.

4.3.Zone de contrôle partagé

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

En grandes lignes, la racine est mise à jour dans une séquence :

- l'ICANN reçoit des demandes de mise à jour des TLD et les analyse en profondeur pour identifier les 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 arguments à propos de M et N, et de la nécessité / souhait 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 permettre au processus politique de décider comment le contrôle pourrait

être partagé pour commencer. À notre avis, il faudrait créer une boîte à outils pour le contrôle de la zone partagée, non seulement pour la racine, mais aussi pour d'autres problèmes de coordination de zone. Nous faisons remarquer que le groupe de travail des opérations du DNS (DNSOPS) de l'IETF a deux propositions pour coordonner les informations de signature DNSSEC, mais il se demande s'il ne serait pas préférable de créer un système général plutôt que de résoudre ce problème ponctuel. La coordination des adresses avant et arrière pourraient 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 de la zone elle-même, des règles, et des journaux individuels pour que chacun des participants publie ses demandes et ses actions
- Chaque type de demande est visible pour tous les autres participants qui peuvent approuver ou désapprouver ou temporiser
- Les règles définissent ce qui arrive à une demande
    - Un type de règle est un vote qui définit les conditions pour qu'une demande soit réussie. Cela pourrait inclure un retard 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) dicteraient 1 de N, de sorte que chaque domaine de premier niveau géographique (ccTLD) pourrait modifier unilatéralement ses propres données.
        - D'autres domaines pourraient utiliser la majorité simple
    - Les délais indiqués pourraient être importants pour que d'autres soient en mesure de signaler les problèmes opérationnels et de laisser aux demandeurs la possibilité de reconsidérer la question
    - Des conditions différentes peuvent s'appliquer pour différentes opérations, comme la création d'une nouvelle édition de rapport, etc.

Par la suite, les participants pourront faire un algorithme standard pour générer un état cohérent. Cela peut sembler une fantaisie, mais les algorithmes byzantins comme Bitcoin [Andreesen 2014] et Namecoin montrent que ces systèmes sont possibles aujourd'hui.

(Notez que nous ne proposons pas les règles, tout juste 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 sur laquelle il pouvait 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 de TLD, par exemple les étiquettes réservées dans plusieurs langues. Tous ces paramètres doivent être mis à disposition en ligne, peut-être dans le DNS, et certainement de manière sécurisée, afin que toute la communauté Internet puisse les utiliser.

4.5.2. Anniversaire des domaines, activités et bailliages

La réputation du DNS est un outil de sécurité important. La date de création d'un nom de domaine est peut-être la pièce d'information la plus indicative. Le taux de mise à jour d'un domaine pour les noms de serveur et les adresses l'est aussi. Les nouveaux domaines et une forte activité de mise à jour sont suspects. Il serait souhaitable que cette information soit disponible en temps réel.

L'information de bailliage a été discutée de façon similaire, mais la question sera reprise par l'IETF dans sa prochaine réunion de mars 2014 à Londres.

4.5.3. L'exemple LISP

Au tout début, on a demandé au panel de considérer la possibilité d'avoir un service super-racine soutenu par l'ICANN 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. Nous avons trouvé les ressources de quatre serveurs, mais le projet n'a jamais pu démarrer en raison de certaines questions non résolues :

- quelle serait la portée (durée, etc.) de l'expérience ? Quels 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-il s'occuper de la question ou serait-ce du ressort des registres Internet régionaux (RIR) ?
- la réponse serait-elle différente si les adresses IP n'étaient pas impliquées ?

Les documents de LISP sont joints en annexe. 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 en tant que telle, ne présente aucune nouvelle tâche de gestion de l'identificateur qui soit en dehors des pratiques actuelles de gestion opérationnelle de

l'identificateur, et en conséquence, le fait que cette forme particulière de tunnellisation exige une attention particulière et un soutien de l'ICANN n'a pas été clairement attesté ».

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

4.6. Collision

Beaucoup de membres du panel étaient familiarisés avec la question de la collision du DNS, et bien que de nombreuses discussions sur la question aient eu lieu, aucune nouvelle recommandation substantielle n'est apparue. Le panel trouve que le prototypage du monde réel du système décrit dans [ICANN 2013] est fortement recommandé.

5. Fondements du protocole DNS

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

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, nous présentons 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 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 reçoivent pas de courrier ni de trafic Web. Mais sur les quelque 60 types d'enregistrement qui ont été définis, moins de 10 sont largement utilisés.

Les efforts pour créer une application ont été confrontés à des difficultés similaires.

La première série d'appels à commentaires (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 de normes concurrentes pour l'authentification du courrier électronique a conduit à deux mises en œuvre en utilisant TXT RR, et à un débat pour savoir si la normalisation de nouveaux types serait toujours utile.

L'effort du système E.164 NUMber mapping (ENUM) pour normaliser le téléphone et d'autres routages de média à l'aide du DNS a également eu un succès très limité. Même si la technologie Name Authority Pointer (NAPTR) 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 de 576 octets (MTU) a probablement fait plus pour retarder le DNS que tout autre facteur ; le DNSSEC et le mécanisme d'extension pour DNS (EDNS0) ne correspondent pas ; toutefois, beaucoup de matériel et de logiciel ne peuvent pas faire passer de grands paquets.
- préserver la connectivité
- essayer d'encourager les 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
- fournir des encouragements pour l'adoption

5.2.Modèle de données

Les premières 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 de l'enregistrement TXT générique destiné à des chaînes de texte arbitraires pour transporter les données avec un autre niveau d'étiquette comme substitut pour le type RR.

Nous dirions que le DNS devrait définir ses propres types de RR et les formats 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 des objets de données auto-signés qui peuvent exister indépendamment du nom de domaine.

5.3. Distribution

La structure de la zone de données et la mise en cache par l'enregistrement de ressource est mise 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 avec des numéros de série qui pourrait rafraîchir les groupes de données mises en cache sans transférer réellement les données.

Nous pensons également que la sécurité pourrait être améliorée par la mise en place de réplication plus fréquente de zones (possiblement plus petites). Ces données n'ont pas besoin d'être sécurisées par le DNSSEC, et peuvent donc améliorer la sécurité là où le DNSSEC n'est pas mise en œuvre.

5.4. Interface de programmation d'applications (API)

L'API DNS existe sous deux formes : une interface utilisateur et des noms au niveau de l'API. Dans les deux cas, nous pouvons bénéficier d'une syntaxe standard qui permet 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 révisions qui, pour la plupart, se sont avérées des échecs. Récemment, Paul Hoffman a fait une présentation sur un nouveau projet, avec des interfaces asynchrones et le soutien du DNSSEC. Voir annexe. Nous savons que le travail est actuellement en cours à Verisign Labs et NLnet, mais nous n'avons pas été en mesure d'obtenir de plus amples renseignements, bien que la publication soit imminente.

Mais indépendamment de l'API, il y a une question connexe à propos de l'endroit où la validation du 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, tandis que chaque utilisateur ne peut pas choisir le filtrage DNS, 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 un autre service.

Les contraintes politiques et juridiques peuvent dire le contraire.

Protocole de requête

5.5. Protocole de requête

Le protocole de requête DNS aborde deux types de questions : premièrement, celles relatives au transport des requêtes / réponses d'un demandeur à un serveur, et deuxièmement, l'élargissement de la puissance de la requête.

Les questions de transport UDP originales commencent par la limitation traditionnelle de l'unité de transmission maximale de 576 octets (MTU). La correction initiale était de revenir 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 limites de l'unité de transmission maximale ont eu un impact très répandu menant à la limite 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 limites telles que la taille 1582 de trame Ethernet ou les 1280 d'IPv6, etc., qui limitent fondamentalement l'UDP.

Aussi, 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 limiter la taille des paquets, ou même intercepter les requêtes DNS dans des proxys transparents, souvent au détriment du service. Des problèmes similaires peuvent exister dans la mise en cache des serveurs de noms qui ne supportent pas les 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 d'entretien normal, lorsque les paquets sont légèrement plus grands.

Les attaques DNS DDOS 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 permettrait de résoudre une partie importante du problème, aussi bien pour le DNS que pour de nombreux autres protocoles. Le panel soutient cette possibilité 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.

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 du trafic Web sécurisé, et cette voie serait une garantie (certains disent que c'est la SEULE voie pour garantir le trafic). Le prix est l'état de connexion et les frais généraux connexes. Les alternatives impliquent un nouveau protocole de transaction ou une nouvelle façon d'utiliser l'UDP. Mais les deux peuvent 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.

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

6. Observations et recommandations

- L'utilisation du DNS dans l'infrastructure va continuer de s'accroître ; l'utilisation du DNS dans l'interface utilisateur (UI) est contestée par des alternatives basées sur la recherche, des interfaces mobiles, etc.

- L'ICANN devrait publier plus de données signées DNSSEC pour les étiquettes réservées, etc.
- En coopération avec l'IETF et autres, faire une étude pour définir une vision architecturale pour le DNS en 2020.
- Publication de racine ouverte de prototype et conception.
- Concevoir un système de contrôle de la zone partagée pour la racine.
- Effectuer des exercices de collision pour tester 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

[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

AI Intelligence artificielle

API Interface de programmation d'applications

CCN Réseau informatique basé sur les contenus

ccTLD Domaine de premier niveau géographique - TLD attribué à un pays en particulier

DANE Authentification des entités nommées basées sur le DNS

DDOS Déni de Service distribué

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

Opérations DNSOPS 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 domaine 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

IP – Protocole Internet

IPSEC Protocole de sécurité IP

IPv4 Protocole Internet version 4

IPv6 Protocole Internet version 6

ITI Panel sur l'innovation technologique - 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) sur une interface

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 Name Authority Pointer - Un type de données DNS couramment utilisé dans la téléphonie sur Internet

NDN Réseau informatique basé sur les informations

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 le Canada, les 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 de l'information dans le DNS

TSIG Signature de transaction

TTL Temps à vivre

TXT Le texte du type RR qui permet les champs de texte de format libre

UDP Protocole de datagramme utilisateur – Protocole de télécommunications sans connexion utilisés 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 textuelles et rapportées 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 décentralisé sont complexes pour moi.

Toutefois, il n'existe pas de systèmes d'identification décentralisés mais coordonnés qui, à ma connaissance, soient en fait largement utilisés actuellement. Alors, que cela nous plaise ou non, le système DNS reste un des système d'identification déployé que nous avons. Comme nous le faisons à l'IETF, les « codes de fonctionnement » gagnent mais cela ne signifient pas qu'ils soient les mieux conçus.

Je ne crois pas en une racine multiple, ou 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 cette 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 ; en échange, cela augmente la complexité technique

ICANN

Le DNS et la nature centralisée de la racine sont en quelque sorte le résultat de la simplicité d'utilisation de la fonction IANA d'origine qui est devenue l'énorme organisation appelée 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 d'exécution » 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, et surtout, il pourrait être mieux mais il 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. Finalement, il doit y avoir quelqu'un ou une organisation qui s'occupe de la coordination mais, à ce moment-là, nous nous trouverons face 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 sorte à pouvoir incorporer une communauté plus large. Dans un certain sens, le travail que nous avons fait sur les IDN concerne un groupe de la communauté d'utilisateurs qui a besoin d'utiliser sa propre langue maternelle dans l'écosystème DNS, au lieu de les laisser construire leur propre système.

Alors que certains me disent que si nous avions fait IDN en dehors de l'écosystème DNS, le déploiement aurait pu être beaucoup plus rapide (voir, par exemple, Mots-clés des langues autochtones), je dis que l'IDN est également mieux car il fait partie de l'écosystème DNS, où il y a des standards ouverts bien définis, des implémentations ouvertes, des compagnies qui se basent sur la légitimité du DNS, et aussi la protection des titulaires d'IDN et des utilisateurs finaux.

Dans ce sens, je n'ai aucun doute et je soutiens la possibilité d'explorer la façon dont nous pouvons étendre le DNS dans les identificateurs étant donné qu'à l'origine il n'était pas 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 de DNS et de l'ICANN.

Politique relative à la racine

La politique de l'ICANN, et le nombre d'opinions de l'ICANN dans le cadre de la « gouvernance de l'Internet » viennent du rôle de l'ICANN dans la coordination des serveurs racine.

Pour compliquer encore les choses, 11 des 13 serveurs racines 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 et en disant qu'il n'y a pas moyen d'étendre au-delà de 13 racines.

Je peux accepter l'argument historique.

Mais je ne peux pas accepter les arguments techniques. C'est plutôt une excuse parce que je n'ai pas connaissance que l'IETF ait étudié sérieusement la façon d'étendre les racines 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 / 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 racines n'est pas si central.

Le fait d'avoir une racine ne signifie pas avoir immédiatement le contrôle de l'Internet. De fait, c'est aussi ennuyeux qu'une racine Anycast. Bien 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.

Donc, il y a des considérations lors de la sélection d'un opérateur de serveur racine, car il est primordial à 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 de 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)	aucun	aucun	jamais
Firefox (25.0)	jamais*	toujours	jamais

Opera (17.0)	aucun	aucun	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 sur la cohérence et la contribution de la dérive - Geoff Huston

Si l'on remonte en arrière en analysant les origines du système de noms de domaine, on trouve ce qui a été appelé le « fichier hosts », une première tentative de mettre les noms de l'activité humaine dans le contexte des réseaux informatiques. L'ARPANET utilisait un modèle de nomination de nœud de 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. Il n'y avait pas d'uniformité imposée à travers 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 compréhensibles par l'homme à la place des adresses de niveau de protocole plus obtus. 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. Comme l'ARPANET a augmenté, tout comme la taille et le taux de mise à jour du fichier hosts, et les frais correspondant à la maintenance de la précision des hôtes locaux ont également augmenté. Le format de fichier hosts a été normalisé (RFC952) et un service de fichier hosts central pouvant prendre la place de nombreuses copies locales du fichier hosts a été défini (RFC953).

Cela fut alors remplacé par le système de noms de domaine (DNS), spécifié à l'origine, en 1983, dans le RFC 882 et le RFC 883 . Le mécanisme de traduction d'un nom – spécifié comme une chaîne conviviale à l'homme– à une adresse de service spécifique au protocole a été maintenu dans la transition du fichier hosts au DNS.

Cet espace d'identification possède un certain nombre de propriétés, y compris l'observation que le DNS s'étend sur un espace de nom qui convient pour une utilisation dans le discours humain, tout en admettant une structure formelle suffisante pour permettre aux noms d'être manipulés par des

applications informatiques de manière déterministe. L'espace de nom DNS est un espace de la structure hiérarchique, permettant de chercher avec efficacité dans l'espace de nom pour trouver des correspondances exactes, et en même temps permettre d'avoir un cadre de gestion distribué de l'espace de nom. Tant que les collisions d'étiquettes sont évitées dans une zone individuelle de la hiérarchie du nom DNS, les collisions de noms peuvent être évitées dans l'espace global de noms DNS, permettant à l'unicité du nom d'être facilement gérée dans le cadre du DNS. Le DNS est flexible en termes de fonction de cartographie et peut être utilisé pour élaborer de la carte d'un espace de nom structuré à toute autre forme de ressources nommée que notre service désigne. Le DNS est destiné à être cohérent car, compte tenu d'une entrée de nom cohérent dans le DNS, les requêtes de ce nom devraient fournir la même réponse sur différentes destinations de l'émetteur de requêtes et à différents moments de la requête. Cela permet une cohérence référentielle, dans le mesure où un nom DNS peut être passé entre les parties et se référer à une ressource cohérente de l'emplacement du service. Le DNS n'est pas destiné à remplacer un système de répertoire ou un système de recherche. S'il y a une correspondance exacte du nom interrogée dans le DNS, la requête DNS renverra la valeur cartographiée comme résultat de la requête, sinon, la requête donnera un échec d'assortiment.

Ce modèle de l'espace de noms DNS a depuis subi un certain nombre de changements comme espace de nom de l'identificateur utilisé pour soutenir une interface humaine avec le réseau , principalement en réponse au mode d'utilisation humain des identificateurs dans le discours. Nous avons tendance à utiliser des identificateurs de façons moins précises et d'une manière qui comprend des éléments de contexte local, qui utilisent les langues et les écritures locales, et au fil du temps le rôle du DNS comme forme de l'interface humaine avec les ressources et les services du réseau a été intégré par les efforts pour soutenir des interfaces qui agissent d'une manière plus « naturelle » pour une utilisation humaine.

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 de l'étiquette, ce qui permet à l'utilisateur de spécifier la partie initiale d'un nom de domaine, et de relayer sur l'application locale ou sur les routines logicielles de résolution de nom pour ajouter un suffixe défini localement pour former un nom DNS complet.

Cette forme d'occlusion sélective de l'espace d'identificateur de DNS grâce à l'utilisation de suffixes de noms a été menée un peu plus loin dans l'interface utilisateur fournie par les navigateurs web, où la pratique courante avec les navigateurs web était de prendre le composant identificateur DNS d'un URL et d'appliquer une transformation de nom en faisant précéder la chaîne de “www.” et en ajoutant un suffixe défini localement (généralement “.com.”) . De cette manière, l'identificateur que l'utilisateur a spécifié et le nom de l'identificateur utilisés dans la requête DNS ultérieure étaient liés, mais n'étaient pas nécessairement les mêmes.

Cette utilisation des transformations de noms au niveau local a été étendue 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 entré par l'utilisateur est transformé en une chaîne étiquette codée qui fait la requête DNS. Dans ce cas, la transformation est définie avec précision, de sorte que plusieurs implémentations de la norme IDN sont destinées à soutenir une vision cohérente de la cartographie d'un identificateur dans un script donné et à une forme de nom DNS codée.

Une autre évolution du raffinement du modèle de l'interaction humaine était l'unification des termes de recherche et d'URL en tant qu'ajout aux 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 dater.

9.4.Contribution de Paul Vixie

Anycast universel pour la zone racine

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 signifie une zone racine dont les enregistrement NS du sommet listent seulement deux des 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 inclut des tests publics à large échelle de services de nom de racine IPv6 - seulement et des tests publics à grande échelle des effets de collision des « nouveaux gTLD ». Cette approche traite le service de nom racine comme un utilitaire non géré plutôt que comme un utilitaire géré.

Contexte

Anycast universelle pour la zone racine ne pouvait pas être déployée de manière sûre et responsable avant l'avènement de DNSSEC, car sans DNSSEC, tout serveur répondant pouvait être configuré avec les données de racine DNS arbitraires y compris les nouveaux TLD ou les TLD redélégués existants. Avec le DNSSEC, il est désormais possible pour les opérateurs de serveurs de noms récursifs de configurer la validation DNSSEC; toutes les informations gTLD entendues d'un serveur de nom racine anycast universelle doivent être approuvées par IANA, comme indiqué par les signatures DNSSEC faites avec la clé de signature de zone racine de l'IANA (ZSK).

Les critiques du système de serveur de noms de racine actuel et historique comprennent son manque de résistance à une attaque DDoS, et le fait que même avec l'anycasting actuel de large échelle par tous les opérateurs de serveur de l'opérateur de nom de la 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 serveur de nom racine soit nécessaire même pour la communication purement locale nous préoccupe aussi, car les clients non locaux n'ont aucun moyen de découvrir les services locaux. Dans un monde basé sur un système distribué et dimensionné comme l'Internet, les services essentiels doivent être extrêmement bien distribués.

Détails

Il existe plusieurs variantes utiles pouvant être construite. Tout d'abord, l'anycast universelle de base permettra à tout opérateur de serveur de nom de capturer le trafic dirigé vers le système de serveur de nom racine et d'y répondre localement. IANA génère et signe numériquement (avec le DNSSEC) une version supplémentaire de la zone racine qui a 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. IANA demande les micro-attributions d'infrastructure d'un registre internet régional (RIR) (tels qu'ARIN ou APNIC), comme plusieurs préfixes de IPv4 24 bits et plusieurs préfixes IPv6 48 bits, pour une utilisation dans 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 IPv6 uniquement.

Une troisième variante de la zone racine actuelle fournirait une anycast universelle comme ci-dessus, mais inclurait les délégations de tous les nouveaux gTLD connus, y compris ceux qui ne sont pas prêts pour la délégation (tels que .CORP et .HOME). Ces nouveaux gTLD seraient délégués à un serveur de nom opéré par l'IANA lui-même, à des fins de mesure. À chaque nouveau gTLD sera attribué des enregistrements A et AAAA wildcard (ou Joker DNS), dont les adresses atteindront des serveurs Web exploités par l'IANA à des fins de mesure.

Impact

Étant donné la nature hiérarchique du routage de l'Internet, des blocs d'adresses anycast peuvent être annoncés à plusieurs niveaux. Une machine virtuelle (VM) en cours d'exécution sur un ordinateur portable peut avoir son propre processus de serveur de noms qui écoute sur les adresses connues appropriées, dans ce 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 servirait d'autre 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 sur ces adresses, dans ce cas, aucune requête du serveur de noms racine ne quittera ce LAN sans fil. Le FSI pourrait faire fonctionner des serveurs qui écoutent sur 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 serveur 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 de cela serait des capacités de diagnostic réduites, et la vulnérabilité accrue aux « empoisonnement de route » ou « détournement » du trafic du service de

noms racine. Il est en tout cas essentiel que la validation DNSSEC devienne commune afin de réduire les représailles pour 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 de l'enregistrement NS sommet pour chaque variante de la zone racine , y compris la colle (glue) de l'adresse. Ces données seraient incluses dans une zone de racine de variante avant la signature du DNSSEC et publiées comme fichier « indications de racine ». 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 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

gtldstudy-2 IN AAAA 2001:?:6::2

gtldstudy-2 IN A ?.?.6.2

10. Annexes

10.1. Documents LISP