DNS : l'architecture qui a failli ne jamais exister

Stéphane FOSSE
fosse.fr

13 janvier 2026

Résumé

En 1983, deux ingénieurs de l'University of Southern California, Jon Postel et Paul Mockapetris, créent le Domain Name System pour résoudre une crise. Le fichier HOSTS.TXT, qui référençait tous les ordinateurs d'Internet depuis 1972, devenait ingérable. Leur solution reposait sur une idée simple : distribuer l'autorité plutôt que centraliser l'information. Ce choix d'architecture, dicté par les contraintes techniques de l'époque, allait déterminer la structure politique d'Internet pour les décennies suivantes.

Avant le DNS, Peggy Karp avait conçu en 1971 un système de « mnémoniques d'hôtes » documenté dans la RFC 226 [1]. Chaque machine du réseau ARPAnet recevait un nom lisible, mappé à son adresse IP dans un fichier texte unique. Le Stanford Research Institute (SRI) maintenait ce fichier HOSTS.TXT et le distribuait via FTP. Les administrateurs envoyaient leurs modifications par email, le SRI compilait les changements, et chaque site téléchargeait la nouvelle version. Le système fonctionnait.

Jusqu'à ce que le réseau change de nature. L'ARPAnet d'origine connectait quelques dizaines de gros systèmes de temps partagé, un par organisation. Avec l'arrivée des réseaux locaux et des stations de travail au début des années 1980, le nombre d'hôtes explosa. À Berkeley, on ajoutait trois nouvelles machines par jour ouvré entre janvier 1986 et février 1987 [2]. Le fichier HOSTS.TXT enflait proportionnellement, et chaque téléchargement mobilisait davantage de bande passante. Pire, les collisions de noms devenaient fréquentes : si deux sites choisissaient le même identifiant entre deux mises à jour, l'autorité centrale devait trancher.

1 Le choix de la délégation hiérarchique

David Mills, ingénieur chez COMSAT, publie en 1981 la RFC 799 [3] qui esquisse un système de domaines Internet. Son objectif immédiat était pragmatique : faciliter le routage du courrier électronique entre réseaux hétérogènes. Mais ses concepts dépassaient largement ce cas d'usage. Jon Postel et Zaw-Sing Su du SRI affinent l'idée dans la RFC 819 [4] en 1982, puis Paul Mockapetris publie en novembre 1983 les RFC 882 et RFC 883 [5], [6] qui définissent le DNS tel qu'on le connaît.

Le design repose sur deux mécanismes : la délégation et l'autorité. Une zone représente une portion de l'arborescence des noms que contrôle une organisation. Le propriétaire d'une zone peut créer des sous-zones et en déléguer la gestion à d'autres sans intervention de l'autorité parente. Cette décentralisation résolvait le problème de scalabilité, mais créait un nouveau défi : comment garantir que les données distribuées restent cohérentes et accessibles ?

Mockapetris et ses collègues ont étudié les systèmes existants. IEN116, une proposition antérieure pour l'ARPAnet, leur semblait trop limitée et trop liée à l'architecture matérielle. Les services Grapevine et Clearinghouse de Xerox étaient sophistiqués, mais leur modèle de réplication intensive avec peu de cache ne correspondait pas au style « chaotique » de l'Internet naissant. Importer ce design aurait signifié importer toute la pile protocolaire Xerox. Ils sont partis d'une feuille blanche.

2 L'arbitrage entre cohérence et disponibilité

L'architecture DNS distingue deux types de composants : les serveurs de noms, qui détiennent l'information faisant autorité pour une zone, et les résolveurs, qui interrogent ces serveurs au nom des applications. Cette séparation permet aux organisations de centraliser leur fonction de résolution dans quelques serveurs dédiés, mutualisant ainsi le cache. Un PC sans ressources peut s'appuyer sur un résolveur distant plutôt que d'embarquer toute la logique de résolution.

Le transfert de zone gère la réplication entre serveurs faisant autorité. Dans la première mouture, un serveur maître contrôlait des serveurs esclaves qui interrogeaient périodiquement le maître pour vérifier si les données avaient changé. Ce modèle pull introduisait de la latence. Une décennie passa avant que les RFC définissant NOTIFY et les transferts de zone incrémentaux (IXFR) n'inversent le flux : le maître notifie

désormais ses esclaves quand les données changent, et seules les modifications transitent sur le réseau au lieu de la zone complète.

Le cache constitue la seconde couche de distribution. Chaque enregistrement DNS porte un Time To Live (TTL) exprimé en secondes, qui indique combien de temps un résolveur peut réutiliser la réponse. Des TTL courts garantissent la fraîcheur des données au prix d'un trafic accru. Des TTL longs minimisent les requêtes mais prolongent les périodes d'incohérence transitoire. Les administrateurs fixent ces valeurs lors de la définition de leur zone, arbitrant entre latence et charge réseau selon leurs contraintes. La recommandation initiale pour les noms d'hôtes était de deux jours.

Ce choix de conception supposait que le cache serait bénéfique. Mockapetris et Dunlap ont été surpris par l'ampleur de l'effet. En 1988, les serveurs racine traitaient environ une requête par seconde. Grâce au cache, ce chiffre restait stable même quand le nombre de clients augmentait. Le mécanisme d'*additional section processing* amplifiait l'efficacité : lorsqu'un serveur répond, il inclut dans sa réponse toute information supplémentaire qu'il juge pertinente, tant que le datagramme reste sous 512 octets. Les serveurs racine ajoutent systématiquement l'adresse IP d'un serveur de noms quand ils en communiquent le nom, anticipant la requête suivante. Cette optimisation a divisé le trafic par deux.

3 UDP contre TCP : le pari du datagramme

Le DNS privilégie UDP pour les requêtes-réponses standards. Ce choix surprend : UDP ne garantit ni livraison, ni ordre, ni intégrité. TCP aurait offert une couche de fiabilité bienvenue. Mais l'overhead de TCP était rédhibitoire dans le contexte de 1983. Établir une connexion TCP pour chaque lookup aurait saturé les ressources des serveurs et du réseau.

L'expérience a validé cette décision. Les performances du réseau Internet se sont révélées bien pires que prévues. La multiplication des passerelles au fil de la croissance a créé des pannes de connectivité et des chemins unidirectionnels. Les délais s'allongeaient. Les serveurs racine répondaient en moins de 100 millisecondes, mais les clients observaient des temps de réponse de 500 millisecondes à 5 secondes selon leur position dans le réseau, et jusqu'à 30 ou 60 secondes pour les domaines délégués pendant les heures de pointe. Avec TCP, ces chiffres auraient été catastrophiques.

Le compromis imposait aux implémentations de gérer elles-mêmes la retransmission. Les développeurs devaient estimer des timeouts, décider combien de tentatives effectuer, choisir entre serveurs alternatifs. Beaucoup ont écrit du code « qui marche » sans l'optimiser. Les logs des serveurs racine montraient des clients envoyant des copies identiques de la même requête, signe de stratégies de retransmission agressives ou mal calibrées. Ce trafic inutile représentait environ la moitié de la charge en 1988.

4 Les réponses négatives : un angle mort

Entre 20 et 60 % des requêtes adressées aux serveurs racine en 1988 obtenaient une réponse négative : le nom n'existe pas, ou l'information demandée n'est pas disponible pour ce nom. L'équipe Mockapetris anticipait que ces erreurs seraient rares, liées à des fautes de frappe occasionnelles. Erreur d'appréciation.

Deux facteurs expliquaient ce taux élevé. D'abord, beaucoup de programmes utilisaient encore des noms au format pré-DNS, ou des adresses provenant d'autres internets comme UUCP. Les serveurs de messagerie testaient systématiquement si une adresse appartenait au domaine Internet en interrogeant le DNS, même quand d'autres indices permettaient de le déterminer. Chaque adresse UUCP générait une requête DNS vouée à échouer. Ensuite, l'adoption des « search lists » par les applications a multiplié les tentatives. Un utilisateur tape « serveur » dans son navigateur, le système essaie successivement « serveur.local », « serveur.departement.local », « serveur.entreprise.local » avant d'abandonner. Chaque étape produit une réponse négative.

L'équipe a ajouté le cache des réponses négatives comme fonctionnalité optionnelle. Les implémentations qui l'ont intégré ont constaté des gains de performance substantiels. Cette fonctionnalité est devenue standard par la suite. Le problème initial révélait une leçon plus générale : distribuer le contrôle ne distribue pas l'expertise. Les administrateurs configuraient leurs systèmes jusqu'à ce qu'ils fonctionnent, rarement jusqu'à ce qu'ils fonctionnent bien. Les exemples de la documentation étaient copiés sans réflexion. Un TTL d'une heure, facile à expliquer dans un tutoriel, se retrouvait partout alors que le texte recommandait plusieurs jours.

5 La centralisation par défaut : HOSTS.TXT en filigrane

Le DNS devait remplacer HOSTS.TXT. Il fallait donc que quelqu'un gère la racine et les premiers niveaux. En 1985, la Defense Communications Agency (DCA, devenue depuis Defense Information Systems Agency ou DISA) confie au SRI l'enregistrement des noms de domaine et à l'Information Sciences Institute (ISI) la gestion technique de la racine. Le choix était logique : ces organisations avaient conçu le système.

Les premiers domaines de premier niveau furent définis dans la RFC 920 [7] en 1984 : .com, .net, .org, .edu, .gov, .mil, .arpa pour les catégories organisationnelles, et des codes pays à deux lettres selon la norme

ISO. Un domaine .int était prévu pour les organisations multinationales. Le document envisageait déjà que chaque pays gère son propre espace.

Mars 1985 voit l'enregistrement des premiers noms de domaine, probablement symbolics.com ou think.com selon les sources. Berkeley lance au printemps ses premières machines fonctionnant uniquement avec le DNS, sans copie locale de HOSTS.TXT. À l'automne, les passerelles de messagerie du campus basculent. Toute l'université adopte les adresses au format domaine. La transition fut douloureuse : éduquer les utilisateurs à la nouvelle syntaxe prenait du temps, les adresses obsolètes circulaient longtemps, et les premiers résolveurs manquaient de fonctionnalités pratiques comme les search lists. Mais le besoin était indéniable. En février 1987, Berkeley comptait 1002 hôtes répartis sur 44 sous-réseaux. Un an plus tard, 1991 hôtes et 86 sous-réseaux, organisés en cinq sous-domaines.

À l'échelle globale, environ 300 domaines étaient délégués en février 1987. En mars 1988, plus de 650. Le fichier HOSTS.TXT référençait alors environ 5500 noms, contre plus de 20000 accessibles via DNS. Le basculement s'accélérait, mais HOSTS.TXT resta en service pendant des années pour les systèmes anciens.

6 Treize serveurs racine, une fiction pratique

Le mythe veut qu'il existe exactement 13 serveurs racine. C'est inexact. Il existe 13 adresses IP où trouver des serveurs racine. Derrière chacune de ces adresses se cachent des dizaines, voire des centaines de serveurs physiques distribués géographiquement. Tous stockent une copie du même fichier, qui agit comme « index principal » du DNS en listant les serveurs faisant autorité pour chaque domaine de premier niveau.

Ces serveurs sont consultés moins souvent qu'on pourrait le croire. Une fois qu'un résolveur connaît l'adresse d'un TLD, il la met en cache et ne vérifie que sporadiquement si elle a changé. Les serveurs racine restent néanmoins vitaux. En 1988, sept serveurs redondants assuraient le service, trois sous TOPS-20 avec le logiciel JEEVES et quatre sous Unix avec BIND. En 2019, le trafic typique tournait autour d'une requête par seconde par serveur, avec des pics lorsqu'un serveur devenait indisponible et que le trafic se reportait sur les autres.

Les types de requêtes se répartissaient ainsi : 25 à 40 % demandaient toutes les informations disponibles, 30 à 40 % cherchaient l'adresse IP d'un nom d'hôte, 10 à 15 % effectuaient la résolution inverse (IP vers nom), moins de 10 % concernaient les enregistrements MX pour le routage du courrier électronique. Ces proportions variaient au gré des nouvelles versions de logiciels : une mise à jour défectueuse d'un résolveur populaire a multiplié la charge par cinq pendant plusieurs semaines. Les estimations suggéraient en 1988 qu'environ 50 % du trafic vers les racines aurait pu être éliminé par de meilleures stratégies de cache et de retransmission dans les implémentations clientes.

Les serveurs racine référaient 10 à 15 % des requêtes vers des serveurs de domaines délégués, accomplissant leur rôle d'aiguillage. Les 350 clients distincts identifiés par les mesures de 1988 utilisaient des priorités statiques pour choisir leur serveur racine. Quand l'un tombait, les autres voyaient leur charge augmenter immédiatement. Les opérateurs restaient largement autonomes, mais coordonnaient leurs actions avec ICANN pour maintenir le système à jour.

7 DNSSEC : la sécurité arrive avec quinze ans de retard

Steven Bellovin décrit le cache poisoning en 1990, mais son rapport reste confidentiel jusqu'en 1995. L'attaque exploite une faiblesse fondamentale : rien dans le DNS d'origine ne prouve que les informations reçues sont authentiques et n'ont pas été altérées. Un attaquant peut injecter de fausses données dans le cache d'un résolveur et détourner le trafic vers des serveurs malveillants, intercepter le courrier, rediriger les acheteurs en ligne vers des sites frauduleux.

Les travaux sur une extension de sécurité traînent pendant des années. DNSSEC, pour Domain Name System Security Extensions, repose sur la cryptographie à clés publiques. Chaque zone signe ses enregistrements avec une clé privée, et publie la clé publique correspondante. Les résolveurs peuvent vérifier les signatures pour s'assurer que les données proviennent bien de la source légitime et n'ont pas été modifiées en transit.

L'Internetstiftelsen en Suède, registre du .se, signe sa zone en 2005, devenant le premier domaine de premier niveau au monde à déployer DNSSEC [8]. La preuve de concept aboutit en 2006, et en février 2007, .se propose DNSSEC comme service additionnel à ses registrants. L'objectif était que le service DNS suédois soit non seulement robuste et disponible, mais aussi digne de confiance.

Plusieurs obstacles ralentissaient l'adoption. Les systèmes de gestion de clés et de signature devaient être développés. Aucun produit commercial prêt à l'emploi n'existait, .se a donc construit le sien. Mais offrir DNSSEC au niveau d'un TLD ne suffit pas : chaque propriétaire de domaine doit également avoir un fournisseur de service DNS capable de gérer DNSSEC. Et la valeur réelle n'apparaît que lorsque les utilisateurs finaux valident effectivement les signatures. Typiquement, cette validation est effectuée par le résolveur du fournisseur d'accès Internet. Les principaux FAI suédois ont activé la validation DNSSEC très tôt, donnant un coup d'accélérateur au déploiement.

La signature de la zone racine restait problématique. En 2007, plusieurs registres de ccTLD estimaient que l'absence de racine signée freinait le succès global de DNSSEC, voire le mettait en péril en encourageant le développement d'alternatives incompatibles. Ils ont pressé l'ICANN et l'IANA d'accélérer le processus. La

signature de la racine fut finalement mise en œuvre, mais seulement après plusieurs années de discussions complexes.

8 La guerre des domaines : quand la technique rencontre la politique

En 1991, Government Systems Inc. (GSI) remporte le contrat DDN-NIC auprès de la DISA. GSI sous-traite le travail à Network Solutions Inc., une petite société privée. En mai 1992, NSI répond à un appel d'offres de la National Science Foundation pour gérer les services d'information réseau du NSFnet et du NREN. NSI obtient le contrat en octobre 1992 via l'accord de coopération NSF NCR-9218742. Pour la première fois, la colonne vertébrale d'Internet se retrouve entre les mains du secteur privé.

Jusqu'en 1995, n'importe qui ayant accès à un serveur de noms pouvait enregistrer un domaine gratuitement auprès de l'InterNIC géré par NSI. La spéculation commence : certains enregistrent des centaines ou des milliers de noms dans l'espoir de les revendre. Les noms étaient gratuits, pourquoi se priver ? Cette année-là, NSI introduit une tarification de 50 dollars par nom pour freiner les abus et couvrir les coûts. Le public Internet, habitué aux subventions gouvernementales américaines, proteste. La NSF abandonne finalement les 30 % du tarif qui étaient fléchés vers un fonds d'infrastructure, jugés illégaux car le Congrès n'avait pas approuvé cette taxe. Des centaines de milliers de dollars avaient été collectés auprès de personnes hors juridiction américaine.

La facturation par NSI déclenche une période que certains appellent les « guerres des domaines » [9]. En mai 1996, Jon Postel publie les premiers brouillons sur les iTLD (International Top-Level Domains), s'appuyant sur des travaux antérieurs de Larry Landweber, Randy Bush, Karl Denninger et Brian Carpenter. Ces brouillons visaient deux objectifs : introduire de la concurrence dans l'enregistrement de domaines pour briser le monopole de NSI, et donner à l'IANA le cadre légal et financier nécessaire à sa survie. L'Internet Society (ISOC) adopte la proposition de Postel en mai lors de sa réunion annuelle à Montréal.

En octobre 1996, l'Internet Ad Hoc Committee (IAHC) se forme. Son conseil lit comme un bottin mondain d'Internet : l'ITU (Union internationale des télécommunications), le WIPO (Organisation mondiale de la propriété intellectuelle), l'INTA (International Trademark Association), l'ISOC, l'IANA, l'IAB. En février 1997, l'IAHC annonce la création de sept nouveaux domaines de premier niveau : .firm, .store, .web, .arts, .rec, .info, .nom. Le plan prévoit également un groupe de registrars concurrents organisés en consortium, CORE, et un comité de supervision intérimaire, l'IPOC, qui céderait plus tard la place à un POC permanent. L'ensemble serait formalisé par un gTLD-MoU (Memorandum of Understanding).

Le gTLD-MoU, publié le 4 février 1997, cristallise les oppositions. Certains le jugent trop complexe et impraticable. D'autres s'inquiètent de la dimension internationale des arrangements : le registre serait géré par une association suisse (CORE), la résolution des litiges par le WIPO basé en Suisse, et les activités administratives soutenues par l'ITU, également suisse. Les craintes d'un gouvernement mondial sous l'égide de l'ONU émergent.

Pendant ce temps, des voix dissidentes se font entendre. Karl Denninger et Eugene Kashpureff créent eDNS, une tentative de construire un espace de noms racine alternatif. L'initiative tourne court, Denninger se retire après des désaccords avec Kashpureff. Ce dernier escalade et, en juillet 1997, détourne le DNS d'InterNIC.net pour rediriger le trafic vers AlterNIC, son véhicule de protestation contre le monopole de NSI. Il finit par fuir au Canada où il est emprisonné trois mois en attendant son extradition. De retour aux États-Unis, il s'en tire avec une amende de 100 dollars et une mise à l'épreuve.

Le 17 juillet 1997, une erreur humaine chez Network Solutions corrompt les fichiers de zone maîtres pour .com, .net et .org. Le problème est résolu en quatre heures, mais les répercussions se font sentir pendant plus d'une journée. L'incident survient la même semaine que le détournement d'InterNIC par Kashpureff et fait la une du New York Times. Tout le monde réalise soudain qu'Internet n'est pas aussi indestructible qu'on le croyait. La stabilité du réseau repose largement sur Network Solutions.

Face à cette incertitude, le président Clinton charge le secrétaire au Commerce de « privatiser, introduire de la concurrence et promouvoir la participation internationale » dans le système de noms de domaine. Le Département du Commerce lance le 2 juillet 1997 un appel à commentaires sur le cadre global du DNS, la création de nouveaux TLD, les politiques pour les registrars et les questions de marques. C'est la première fois que le gouvernement américain démontre publiquement une conscience de ces sujets ésotériques. C'est aussi le premier signal que l'accord poussé par l'IAHC n'est peut-être pas « bouclé ».

9 Le Green Paper et la prise en main gouvernementale

Le 30 janvier 1998, Ira Magaziner, conseiller principal du président Clinton pour le développement des politiques, publie un document de discussion qui sera connu sous le nom de « Green Paper ». Selon Jonathan Weinberg, proche du dossier à l'époque, le gouvernement américain pensait pouvoir concevoir une institution qui fonctionnerait mieux. Magaziner avait l'autorité du président pour s'assurer que le contrôle américain du DNS serait maintenu.

Le Green Paper ressemble aux brouillons iTLD de Postel, mais avec une distinction cruciale : le gouvernement américain resterait impliqué à court et moyen terme pour assurer une transition ordonnée vers une nouvelle organisation à but non lucratif, baptisée NewCo. Cette position démolissait le rôle de l'ISOC comme pilote du processus IAHC/gTLD-MoU. Le document s'opposait également aux mécanismes de résolution des litiges de marques que le WIPO avait intégrés au gTLD-MoU. Magaziner soutenait la protection des marques, mais estimait que les registrars, pas NewCo, devaient supporter les coûts et les responsabilités des litiges.

Magaziner annonçait aussi la fin programmée de l'accord de coopération entre Network Solutions et le gouvernement. NSI devait séparer clairement son activité de registre et de registrar, opérer .com, .net et .org en mode registre partagé ouvert à tous les registrars, et transférer .edu à une entité à but non lucratif. Le registre devrait traiter tous les registrars de manière non discriminatoire et facturer les services selon une formule convenue pendant une période transitoire. NSI devait développer la capacité technique de partager l'enregistrement de ses TLD avec n'importe quel registrar dans un délai précis. NSI devait fournir au gouvernement une copie de toutes les données, logiciels et licences de propriété intellectuelle générées sous l'accord, pour usage par la nouvelle corporation au bénéfice d'Internet. NSI devait céder le contrôle du serveur racine « A » et la gestion du système de serveurs racine sur instruction du gouvernement. NSI devait accepter les exigences définies par le Green Paper pour les registres et les registrars. Le monopole de NSI devait prendre fin le 30 septembre 1998.

Pour la première fois, une indication claire venait des plus hautes sphères : le monopole accordé par le gouvernement à NSI avait une date d'expiration. Les détracteurs du processus IAHC/gTLD-MoU avaient désormais une proposition unifiée autour de laquelle se rallier. Les partisans de l'« Old Guard » se retrouvaient avec un plan en lambeaux. Network Solutions faisait face à une limitation sévère de son pouvoir et de ses profits. Et Jon Postel n'était pas satisfait.

Postel publie une déclaration : « Je suis d'accord avec le thème principal de la proposition... Je suis moins à l'aise avec les détails concernant la manière dont les nouveaux gTLD, registrars et registres seraient établis, et la restriction à seulement cinq nouveaux gTLD. »

Le week-end précédant le 4 février 1998, Jon Postel entreprend ce qu'il qualifie de « test du plan de transition ». Il reconfigure le système DNS racine pour obtenir les informations non pas du serveur racine « A » opéré par Network Solutions, mais d'un serveur qu'il opère à l'ISI. Dans une déclaration écrite, Postel explique : « Je voulais voir avec quelle facilité la gestion des serveurs racine pouvait être transférée à une autre machine quand le gouvernement abandonnera son contrôle du système de domaines comme décrit dans le Green Paper. » Le gouvernement américain réagit très mal. Becky Burr, une responsable du Département du Commerce, déclare que le gouvernement n'était au courant de rien. « Le timing est malheureux », ajoute-t-elle, faisant référence à la publication du plan controversé.

Le contrôle du DNS revient rapidement à Network Solutions et donc au gouvernement américain. Mais Postel a clairement montré qu'il était mécontent des déclarations du Green Paper et qu'il était toujours maître du DNS, quel que soit le détenteur du contrôle contractuel.

Le 5 juin 1998, Magaziner publie une version révisée du Green Paper qui prend en compte les nombreux commentaires publics reçus depuis la première version. Ce nouveau document, le « White Paper », est publié comme déclaration officielle de politique du Département du Commerce. Le point le plus pertinent est l'appel de Magaziner à établir un consensus sur les questions présentées par les parties prenantes concernées. Il accorde à Internet une dernière chance de déterminer à quoi ressemblera son destin sous le White Paper.

Plusieurs groupes se précipitent pour s'organiser et forger un consensus. L'International Forum for the White Paper (IFWP) émerge rapidement. Ce forum gagne du soutien pour plusieurs raisons. Il prend de l'ampleur à un moment où le processus IAHC/gTLD-MoU/CORE perd de la vitesse. Chaque groupe qui s'était senti exclu du processus IAHC est spécifiquement accueilli par l'IFWP. Network Solutions soutient l'IFWP, ce qui lui confère une crédibilité que l'IAHC n'avait pas. L'IFWP organise des ateliers régionaux dans le monde entier pour aborder les questions soulevées par le White Paper.

Entre juin et août 1998, Jon Postel rédige une nouvelle série de projets de statuts pour une « nouvelle IANA » qui satisferait au rôle défini par le White Paper. La nouvelle IANA aurait « des responsabilités dans trois domaines interdépendants : les adresses de protocole Internet, les noms de domaine et les paramètres de protocole. Cela inclura le système de serveurs racine et le travail actuellement effectué par l'IANA existante. » L'objectif de la nouvelle IANA était de « préserver les fonctions de coordination centrale de l'Internet mondial pour le bien public ». Postel publie ces brouillons tout au long de juin, juillet et août. Le plus important est publié le 17 septembre avec le soutien de Gabe Battista au nom de Network Solutions. Cette itération est caractérisée comme « les meilleurs éléments des brouillons antérieurs et incluant de larges contributions des parties prenantes et utilisateurs d'Internet tout en restant fidèle aux principes directeurs énoncés dans le White Paper du gouvernement américain. » L'objectif de ces nouveaux brouillons était de « capturer les meilleures idées de toutes les sources, y compris l'International Forum for the White Paper (IFWP), la communauté d'affaires, la communauté technique Internet et d'autres parties prenantes. » Ce projet est connu de la communauté sous le nom d'IANA/NSI Draft 4. Le Draft 5 suit quelques semaines plus tard, le 28 septembre, curieusement, sans le soutien explicite de Network Solutions.

10 La mort de Postel et la naissance d'ICANN

Le 1er octobre 1997, le NTIA annonce que NewCo s'appellera Internet Corporation for Assigned Names and Numbers, ou ICANN. Ce même jour, l'accord de coopération entre le gouvernement américain et Network Solutions devait se terminer et la transition vers ICANN devait commencer. Jon Postel se concentre désormais principalement sur le fait de s'assurer que la transition vers ICANN se fera dans des conditions acceptables et équitables pour tous.

Le 7 octobre 1998, Joe Sims, l'avocat de Postel, comparaît devant le sous-comité de recherche fondamentale et le sous-comité de technologie du comité des sciences de la Chambre des représentants au nom de Jon. Postel, récemment tombé malade, est incapable de témoigner en personne. Le témoignage de Postel inclut une simple déclaration décrivant ses sentiments actuels : « La plupart du travail à venir sera effectué par d'autres ; l'IANA continuera son travail technique et je resterai bien sûr impliqué dans le processus, mais il est temps qu'ICANN commence à diriger cet effort. » Ses mots, bien que simples, annonçaient bien plus que quiconque ne pouvait l'imaginer.

Le 16 octobre 1998, Jon Postel décède.

Avec Jon hors du circuit, le processus vacille quelque peu. Cependant, ayant posé la majeure partie des fondations avec la rafale de brouillons produits plus tôt dans l'année, d'autres sont en mesure de reprendre là où il s'était arrêté. Tout au long du reste d'octobre et de la majeure partie de novembre, Esther Dyson, Joe Sims, Mike Roberts et d'autres travaillent à satisfaire les commentaires émis par le NTIA sur les brouillons de l'IANA. Le 25 novembre, le Département du Commerce des États-Unis annonce qu'il a finalisé les négociations avec NewCo et le reconnaît officiellement comme Internet Corporation for Assigned Names and Numbers dans le but de transférer la gestion du DNS du gouvernement américain à l'industrie.

Gabe Battista démissionne de son poste de PDG de Network Solutions mi-novembre et Ira Magaziner part fin décembre. Il semble qu'il reste très peu de personnes debout en dehors du nouvel ICANN. Bien qu'ICANN ait survécu aux guerres des domaines et ait été jugé digne d'assumer le manteau du Département du Commerce, l'organisation a encore des défis importants devant elle. Maintenant, elle est réellement confrontée à la supervision du DNS, à l'introduction de la concurrence dans l'espace de noms et à l'ajout de nouveaux gTLD à la racine de manière ouverte, transparente et ascendante.

ICANN choisit de poursuivre la mise en œuvre d'un service de registre partagé avec Verisign qui verrait Network Solutions se scinder en deux entités, le registre et le registrar, tandis que de nouveaux registrars concurrents seraient accrédités. Le 25 avril 1999, ICANN annonce qu'elle a sélectionné 34 entreprises qui seront accréditées pour concurrencer Network Solutions dans l'enregistrement de noms de domaine. Cinq de ces entreprises seront autorisées à participer à un banc d'essai spécial conçu pour permettre à un nombre limité d'entreprises de résoudre les problèmes techniques associés au nouveau système de registre partagé que NSI met en œuvre. Le 7 juin, register.com Inc. annonce qu'elle a réussi à enregistrer le premier nom de domaine sous le nouveau régime concurrentiel.

NSI continue de refuser de reconnaître ICANN pendant l'été 1999. Les tactiques fonctionnent raisonnablement bien jusqu'à ce que la situation fasse l'objet d'un examen par une commission d'enquête du House Commerce Committee sur ICANN. Le panel, présidé par Tom Bliley, cuisine Rutt. L'un des échanges les plus rapportés se produit entre Jim Rutt et Bart Stupak, un représentant de la Chambre du Michigan. Stupak demande si NSI a déjà dit à ICANN ou au DoC qu'il n'y avait pas d'accord final. Rutt répond qu'il devra demander à son avocat et revenir le lendemain. Oui, il a dit qu'il n'y avait pas d'accord final. La presse saute sur l'histoire aussi fort que le comité avait sauté sur Rutt.

Entre le 2 et le 4 novembre 1999, la première assemblée générale annuelle d'ICANN se tient à Los Angeles. L'ordre du jour est spécifiquement orienté vers la ratification d'un accord proposé entre ICANN et Network Solutions. Tout le monde convient qu'une trêve est nécessaire, mais peu pensent qu'elle puisse être conclue. Bien qu'ICANN garde une emprise ferme sur les procédures, il y a un nouveau sentiment d'autonomisation parmi certains groupes, le sentiment que tout peut être accompli avec les bons efforts. Il y a une compréhension tacite que cet accord fera ou cassera ICANN. Si les parties n'arrivent pas à une conclusion sur cette question, il est presque certain que la structure se désintègrera.

Le 4 novembre, ICANN et Network Solutions parviennent à une trêve. Entre autres choses, les accords prévoient spécifiquement que Network Solutions devra séparer ses activités de registre et de registrar, qu'elle recevra une prolongation de son accord d'exploitation si elle cède l'une ou l'autre activité dans un délai de deux ans et, plus important encore, qu'elle reconnaît ICANN comme NewCo. Comme prévu, quelques semaines plus tard, le Département du Commerce accepte également ces accords révisés.

L'année suivante se déroule relativement calmement. L'introduction de nouveaux registrars précipite une baisse de prix moyenne de 35 dollars par an à environ 15 dollars. Les taux d'enregistrement augmentent rapidement. ICANN s'occupe de l'introduction de nouveaux domaines génériques de premier niveau. Bien que le processus d'introduction prenne un certain temps, le terrain couvert a été bien parcouru par les débats précédents. Le 16 novembre 2000, le conseil d'administration d'ICANN approuve finalement l'introduction de sept nouveaux domaines de premier niveau : .aero, .biz, .coop, .info, .museum, .name et .pro.

11 Le DNS aujourd'hui : chiffrement et fragmentation

En 2020, le DNS subit sa transformation la plus profonde depuis sa création. Le transport DNS fait l'objet d'une reconstruction. DNS Over HTTPS (DoH), DNS Over TLS (DoT) et le futur DNS Over QUIC (DoQ) remplacent progressivement les requêtes UDP en clair qui caractérisaient le protocole depuis 1983. Ces variantes chiffrées cassent plusieurs traditions du DNS.

Le DNS historique était un protocole ouvert. Toutes les données transitaient en texte clair sur Internet. DNSSEC signe les données mais ne les chiffre pas. Toute donnée dans le DNS accessible publiquement doit être considérée comme publique. Cela ne signifie pas que celui qui accède aux données devrait être public aussi. Beaucoup d'efforts ont été investis pour rendre le DNS plus respectueux de la vie privée.

DoT et DoH sont tous deux chiffrés. Le DNS s'est principalement appuyé sur UDP au fil des ans, à tel point que de nombreux pare-feu ont décidé de bloquer le DNS sur TCP, ce qui est contraire aux RFC actuelles. DoT et DoH se connectent tous deux via TCP à un résolveur, puis établissent une session TLS. DoT transmet toujours de bons vieux paquets DNS. DoH parle HTTP. Ces deux technologies introduisent des changements massifs dans la façon dont le DNS fonctionne. Le changement le plus discuté est l'introduction de « résolveurs de confiance », un concept promu par les fournisseurs de navigateurs.

Le DNS ne reste pas immobile. Il n'y a pas eu une seule réunion de l'IETF où de nouvelles propositions pour de futures fonctionnalités DNS ne sont pas discutées. DNSOP est l'un des groupes de travail les plus anciens de l'IETF et il ne montre aucun signe de ralentissement.

Une menace qui se profile depuis de nombreuses années est l'obsolescence des noms de domaine due aux grands fournisseurs de plateformes comme Google, Facebook ou Amazon. Qui a besoin d'un nom de domaine si vous pouvez être trouvé par Google sans en avoir un ? De nombreuses organisations choisissent de ne pas avoir leur propre domaine et n'ont qu'un compte Facebook. Un grand nombre de commerçants en ligne n'ont pas leur propre boutique et ne sont que des marchands Amazon. Le verdict sur ce modèle commercial est encore à rendre.

Au fil des ans, de nombreuses tentatives ont été faites avec des services de noms alternatifs. Des services racine DNS alternatifs aux services de noms utilisant d'autres technologies, rien n'a pu menacer la domination du DNS tel que nous le connaissons. OpenNIC, un service racine alternatif de longue date, a eu un certain usage au fil des années, mais la grande majorité des utilisateurs n'ont pas accès aux noms OpenNIC. NameCoin, la blockchain la plus ancienne et encore active pour les noms DNS, s'appuie sur la technologie Bitcoin. Tous les noms enregistrés relèvent du TLD .bit, qui n'est pas reconnu par l'ICANN ou l'IETF. C'est exactement le plus gros problème de NameCoin : la majorité des utilisateurs d'Internet n'ont pas accès au TLD .bit. Les blockchains sont actuellement à la mode, et même dans cet espace, des noms stables sont nécessaires. De nombreuses blockchains ont lancé leurs propres services de noms qui ne fonctionnent que sur leur chaîne respective. L'Ethereum Name Service (ENS) s'appuie sur les spécifications DNS des points de code Unicode autorisés dans les noms mais utilise son propre format pour stocker les noms sur la blockchain.

12 Les choix d'hier, les contraintes d'aujourd'hui

Le DNS incarne une tension fondamentale de l'architecture des systèmes distribués. Centraliser garantit la cohérence mais ne passe pas à l'échelle. Distribuer permet la croissance mais introduit des incohérences transitoires et des problèmes de gouvernance. Mockapetris et Postel ont choisi la distribution avec des mécanismes de cohérence éventuelle : zones, cache, TTL. Ils ont fait ce choix dans un contexte où le réseau était lent et les machines limitées. Ce contexte a disparu, mais l'architecture reste.

Les décisions techniques portent toujours des implications politiques. La structure hiérarchique avec délégation d'autorité impliquait qu'il faudrait quelqu'un au sommet. Ce quelqu'un est devenu un enjeu de pouvoir. La capacité de créer de nouveaux TLD, de retirer des domaines, de modifier la racine confère un contrôle considérable. Les guerres des domaines n'ont pas porté sur des questions de latence ou de bande passante, mais sur qui contrôlerait cette infrastructure et comment.

Le cache, présenté comme une optimisation technique innocente, redistribue le pouvoir. Un résolveur qui cache peut voir toutes les requêtes de ses clients, construire des profils d'utilisation, bloquer ou modifier des réponses. Les résolveurs de confiance promus par DoH concentrent le trafic chez quelques acteurs, typiquement Google, Cloudflare, Quad9. Cette centralisation de fait contredit l'esprit de distribution du design original.

DNSSEC ajoute de la sécurité mais aussi de la complexité et de nouveaux points de défaillance. La clé racine KSK, gérée par la PTI via des cérémonies cryptographiques élaborées, devient un point de contrôle unique. Si cette clé est compromise, l'ensemble du DNS signé s'effondre. Les systèmes alternatifs comme NameCoin et ENS tentent de contourner cette centralisation en ancrant la confiance dans une blockchain plutôt que dans une autorité administrative. Mais ces systèmes restent marginaux précisément parce qu'ils ne sont pas compatibles avec le DNS existant. Le coût de migration est prohibitif.

L'histoire du DNS montre qu'une architecture technique détermine bien plus que des métriques de performance. Elle définit qui peut participer, qui peut innover, qui peut censurer. Chaque couche du protocole, chaque choix d'implémentation encode des assomptions sur la confiance, le contrôle, la responsabilité. Ces assomptions deviennent invisibles avec le temps, mais elles continuent de structurer nos pratiques.

Le DNS actuel n'est pas le DNS que Mockapetris et Postel avaient imaginé. Il n'est pas non plus celui qu'auraient voulu les promoteurs du gTLD-MoU, ni celui que Network Solutions aurait préféré, ni celui

que les défenseurs des blockchains réclament. C'est un compromis historique, fruit de trente ans de conflits techniques et politiques. Un système qui fonctionne assez bien pour qu'on ne le remplace pas, mais assez mal pour que beaucoup aimeraient le faire.

Références

[1] P. Karp, Standardization of Host Mnemonics, RFC 226, RFC, BBN, sept. 1971.

[2] P. V. Mockapetris et K. J. Dunlap, « Development of the domain name system », in *Proceedings of SIGCOMM '88*, USC Information Sciences Institute et Digital Equipment Corp., t. 18, août 1988, p. 123-133.

[3] D. Mills, Internet Name Domains, RFC 799, RFC, COMSAT, sept. 1981.

[4] J. Postel et Z.-S. Su, Domain Naming Convention for Internet User Applications, RFC 819, RFC, USC Information Sciences Institute et Stanford Research Institute, août 1982.

[5] P. V. Mockapetris, Domain names - Concepts and Facilities, RFC 882 (obsolète, remplacée par RFC 1034), RFC, USC Information Sciences Institute, nov. 1983.

[6] P. V. Mockapetris, Domain names - Implementation and Specification, RFC 883 (obsolète, remplacée par RFC 1035), RFC, USC Information Sciences Institute, nov. 1983.

[7] J. Postel et J. Reynolds, Domain Requirements, RFC 920, RFC, USC Information Sciences Institute, oct. 1984.

[8] A.-M. Eklund-Löwinder et U. Wisser, « The history and future of the DNS », CENTR 20 Years Anniversary Publications, Internetstiftelsen, rapp. tech., 2019.

[9] R. W. Rader, « One History of DNS », rapp. tech., avr. 2001.

[10] Root Zone Management Review and Computing Systems, IFRT Subgroup Meeting Notes, juin 2020.

[11] P. V. Mockapetris, Domain names - Concepts and Facilities, RFC 1034, RFC, USC Information Sciences Institute, nov. 1987.

[12] P. V. Mockapetris, Domain names - Implementation and Specification, RFC 1035, RFC, USC Information Sciences Institute, nov. 1987.