ICANN81 | Réunion générale annuelle – Comment ça marche : opérations des serveurs racine
Dimanche 10 novembre 2024 – 13h15 à 14h30 TRT

ULRICH WISSER : Bonjour et bienvenue à notre séance « Comment ça marche : opérations des serveurs racine ». Je m'appelle Ulrich Wisser, et je suis le responsable de la participation à distance pour cette séance. Veuillez noter que la séance est enregistrée et qu'elle est régie par les normes de conduite requises par l'ICANN et la politique anti-harcèlement de la communauté de l'ICANN. Au cours de la séance, les questions ou commentaires ne seront lus à haute voix que s'ils sont soumis dans le module Q&R. Si vous souhaitez prendre la parole pendant la séance, veuillez lever la main dans Zoom. Lorsqu'ils seront appelés, les participants virtuels auront la permission de réactiver le son dans Zoom. Les participants sur place utiliseront leurs microphones physiques pour parler. Veuillez indiquer votre nom pour l'enregistrement et parler à un rythme raisonnable. Vous êtes tous invités à utiliser le chat. Veuillez noter que les discussions privées ne sont possibles parmi les panélistes que dans le format webinaire de Zoom. Tout message envoyé par les panélistes ou par un participant standard à un autre participant standard sera également vu par l'hôte de la séance, le co-hôte et les autres panélistes. Je donne maintenant la parole à Ken Renard.

KEN RENARD : Merci. Bonjour. Je m'appelle Ken Renard. Je suis l'un des opérateurs de serveur racine du laboratoire de recherche de l'armée aux États-Unis. Aujourd'hui, nous allons faire une présentation sur l'envie des gens de poser des questions. La séance sera très interactive. Nous sommes heureux que vous soyez ici et de pouvoir partager la façon dont les choses fonctionnent. J'ai un cliqueur. Bref, ce dont nous allons parler aujourd'hui, c'est de quelques DNS, parce que cela nous aide à expliquer comment le système des serveurs racine s'intègre partout. C'est un peu l'état du système des serveurs racine aujourd'hui. Une explication rapide d'Anycast, puis de nous-mêmes et enfin un peu sur leur gouvernance.

Nous commençons donc par le fait que l'adresse IP est vraiment l'identificateur fondamental sur Internet, soit avec ces données numériques, soit avec des chaînes de 1 et de 0 à ces adresses. Donc, si vous êtes connecté à Internet, vous avez une adresse IP. Le problème ici est que nous, humains, on n'est pas très doués pour nous souvenir de ces numéros. Ces numéros peuvent changer beaucoup, et c'est une bonne chose. Voilà, à l'origine, la raison de développer le DNS est d'apporter des numéros et le fait qu'ils changent. La partie la plus moderne est que les adresses IP sont parfois partagées avec plusieurs sites Web sur la même adresse IP. Et il faut savoir qu'une seule adresse, comme un site Web, peut en fait être hébergée sur plusieurs adresses IP. Le DNS est donc notre ami. Il nous facilite beaucoup les choses et il est largement utilisé. Ici, nous avons l'espace de noms. Nous utilisons le DNS pour rechercher des noms dans ces adresses IP. Nous avons donc cet espace hiérarchique de noms qui commence en haut avec une racine. Et en dessous, se trouvent tous nos TLD, ou domaines de

premier niveau. Voici les codes de pays ou géographiques. Voici les gTLD. En dessous il y a le second niveau, ensuite le troisième, etc. Ainsi, l'utilisation probablement la plus courante du DNS est de rechercher un nom dans une adresse IP. Mais il existe d'autres mappages, tels que la recherche de serveurs de messagerie électronique pour un domaine. C'est comme ça que fonctionne le courrier. Il y a souvent des adresses où vous utilisez une adresse IP pour rechercher un nom existant. Il y a aussi beaucoup d'informations de sécurité stockées dans le DNS qui nous aident à mettre en œuvre la sécurité Web. En regardant le DNS, grande déclaration là en bas. Le DNS est une base de données distribuée à l'échelle mondiale, faiblement cohérente, évolutive et dynamique. Pensez-y comme si c'était l'annuaire. Passez un peu de temps avec ça. Il s'agit du processus de recherche d'un nom dans le DNS. C'est le diagramme classique que vous verrez dans presque tous les manuels. Et c'est utile pour décrire les questions de base. Je vais ajouter une couche dessus une fois que nous aurons terminé.

Donc, en regardant le processus, sur le côté gauche, vous avez votre appareil mobile, vous avez votre navigateur Web, votre ordinateur, votre réfrigérateur, votre grille-pain, votre interrupteur, tout ce qui est connecté à l'Internet va agir dans ce rôle pour rechercher des noms dans des adresses IP. Ces noms sont recherchés par votre dispositif avec un résolveur récursif. C'est cette case du milieu. Ces résolveurs récursifs sont le cheval de bataille du DNS global. C'est là que l'on s'amuse le plus. La plupart de l'action se produit là, dans le résolveur récursif. Votre appareil demandera donc au résolveur récursif local l'adresse de, ici nous avons www.example.com. Et ce résolveur récursif va découvrir quelle est cette adresse. Cette action est décrite dans le

processus ici. La première étape est de savoir, où est .com ? Ainsi, le système des serveurs racine n'est que cette boîte en haut à droite. Il va donc poser la question. Le système des serveurs racine va dire, hey, je ne sais pas ce qu'est www.example.com, mais je sais où trouver la base de données .com. Ça va revenir au résolveur récursif. Le résolveur récursif va dire, maintenant qu'il sait comment accéder à la base de données .com, il pose la même question. Et .com répond à peu près de la même manière. Je ne connais pas cette adresse, mais je peux vous dire où est example.com. Cela revient au résolveur, et maintenant le résolveur récursif peut demander la réponse à la base de données example.com, et voilà ce qu'il obtient.

La prochaine partie vraiment importante de tout cela est que le long du chemin, ce résolveur récursif s'est souvenu de chacune des réponses qu'il a obtenues. Votre dispositif vous demande à nouveau cette adresse pour www.example.com. Il connaît déjà la réponse, et il n'a pas à refaire ce processus en trois étapes. Si votre dispositif demande sur q.example.com, il peut sauter la première étape en allant au système des serveurs racine. Il peut sauter la deuxième étape en allant au serveur .com, et aller juste à la dernière. Il y a donc des gains d'efficacité incroyables intégrés dans ce processus. Ces informations sont mises en cache ou mémorisées pendant une certaine période de temps. Spécifiquement pour la racine, les valeurs sont de 48 heures. Alors, pour toutes les fois que vous demandez quelque chose dans .com, votre résolveur récursif doit aller au maximum. Une autre étape de l'efficacité est que vous n'êtes pas le seul à utiliser ce résolveur récursif. Vous et des dizaines, des centaines ou des milliers de vos voisins sur Internet utilisez le même résolveur récursif, de sorte que tout ce que quelqu'un

d'autre a regardé avant peut déjà être mémorisé. Votre dispositif pourrait donc poser des milliers de questions au DNS, et il ne va jamais au système des serveurs racine pour vos transactions, parce que tout pourrait être en mémoire. Sans doute, des gains d'efficacité incroyables ; et voyez ici que le système des serveurs racine, ce serveur racine faisant autorité, est très important parce que c'est le départ, mais il n'est pas utilisé si souvent. Nous passons donc à la suivante.

Un peu plus sur la mise en cache et la résolution. Ainsi, chaque enregistrement DNS a une valeur de temps de validité de la réponse. Cela veut dire combien de temps ce résolveur récursif est autorisé à se souvenir de cette réponse avant qu'elle ne soit jugée suffisamment vieille pour que vous deviez poser la question à nouveau. Ce qui est important, c'est que les serveurs racine ne servent que des informations sur les domaines de premier niveau. Le serveur sait seulement où se trouve .com. Il ne sait pas où se trouve example.com. Juste les domaines de premier niveau. En ce moment, il y a 1450 domaines de premier niveau. Une très petite base de données.

Quelques raffinements modernes maintenant au DNS. Ils ne sont pas spécifiques au système des serveurs racine, mais cela aide le DNS un peu. Pour la sécurité du DNS, il existe les extensions DNSSEC, nous pouvons maintenant signer cryptographiquement les données du DNS. Cela élimine, ou, selon les personnes chargées de la sécurité, réduit le risque d'usurpation. Et ce serveur intermédiaire, ce résolveur récursif au milieu a la capacité de faire le contrôle cryptographique et de vérifier que ce soit réellement correct. Donc, peu importe d'où vous obtenez vos informations du DNS, car vous pouvez réellement vérifier qu'elles

sont correctes et qu'elles n'ont pas été falsifiées. Il y a également des améliorations de la confidentialité. Si vous demandiez www.example.com, nous avons vu que cette question a été envoyée à la racine, elle a été envoyée aux serveurs .com, ainsi qu'au résolveur récursif. Il pourrait vraiment y avoir des informations sensibles là-dedans. Maintenant, du point de vue du système des serveurs racine, nous ne voyons pas l'adresse de votre dispositif, nous voyons seulement l'adresse de ce résolveur récursif. Donc, nous n'avons pas [inaudible] à une machine ou un dispositif spécifique, seulement le résolveur récursif qu'ils utilisent. Il existe d'autres protocoles comme DOT, DNS sur TLS, DNS sur HTTS, DOQ est DNS sur QUIC, qui cryptent en fait le transfert des messages ici. Et, à ce stade ils fonctionnent entre votre dispositif sur le côté gauche et ce serveur intermédiaire, le résolveur récursif. Il reste à voir exactement comment ils seront utilisés dans cette deuxième étape.

Bon, un peu plus sur le système des serveurs racine aujourd'hui. Juste quelques définitions ici, la zone racine. C'est en fait la liste des TLD et de leurs adresses de serveur de noms. Voilà le contenu de la zone racine. Nous, en tant que système des serveurs racine, passons à ça. Nous verrons cela plus tard aussi. Le système des serveurs racine est collectivement l'ensemble des opérateurs de serveurs racine et toute l'infrastructure que chacun des opérateurs déploie à savoir les ordinateurs sur les requêtes Internet. L'opérateur de serveur racine, vous entendrez souvent cela, le RSO, est en fait l'organisation qui gère cette activité et exploite chacun de ces serveurs racine, un peu plus profondément. L'instance Anycast de serveur racine est en fait un emplacement de réseau. Nous avons donc 12 opérateurs de serveur

racine, 13 entités de serveur racine, et 1800 instances Anycast. Ainsi, chaque opérateur exploite de nombreux ordinateurs dans le monde entier sur son adresse IP.

Le Comité consultatif du système des serveurs racine est le comité consultatif de l'ICANN qui est composé de personnes nommées par l'opérateur de serveur racine et certains agents de liaison. Nous fournissons des conseils au Conseil d'administration et à la communauté de l'ICANN sur les opérations de serveur racine. Pour aller un peu plus loin et en quelque sorte séparer l'idée de la zone racine par rapport au système des serveurs racine. Encore une fois, la zone racine est constituée par les données. Le système des serveurs racine est constitué par les ordinateurs qui fonctionnent sur Internet que vous pouvez interroger et qui vous enverront une réponse et répondront à ces questions. Donc une très petite partie du système global. Encore une fois, très important, ces séparations sont intentionnelles pour des raisons de sécurité, pour la séparation des tâches, pour bien établir les rôles et les responsabilités.

Cela ressemble donc un peu plus à la gestion de la zone racine. Si vous êtes un gestionnaire de TLD, vous devrez peut-être changer l'adresse de votre serveur de noms. Cela va à l'IANA. C'est là que ces choses sont modifiées. La base de données réelle est mise à jour. Là on effectue toutes les signatures, et c'est là que le système des serveurs racine commence. Nous obtenons cette table qui est déjà signée, déjà verrouillée, et nous la gérons. Nous envoyons ce fichier à tous nos ordinateurs, tous vos résolveurs DNS sur le côté droit interrogent notre

système. Nous ne sommes qu'une petite partie de la gestion totale de la zone racine.

Nous remontons à 1984, c'est-à-dire il y a 40 ans, lorsque le DNS est né et, à ce moment-là, il y avait quatre serveurs racine. Et comme l'Internet a grandi, le net aux États-Unis ainsi que certains autres, il a fallu les augmenter. Nous avions sept serveurs racine. Nous voyons une grande partie de cette croissance se produire dans les années 80 et 90. Nous avons donc des serveurs racine, pas seulement des opérateurs de serveurs racine qui sont basés dans le monde entier. Chacun de ces opérateurs a des ordinateurs qui existent partout dans le monde. Au fil du temps, nous répondons aux exigences techniques. Il s'agit d'un service technique, et nous avons certains principes qui sont très importants pour que ce système fonctionne. Ça doit toujours fonctionner. Nous répondons donc aux demandes techniques à mesure que la technologie, la demande, les requêtes augmentent au fil du temps. Problèmes de mise à l'échelle. Il y a longtemps, 13 serveurs racine signifiaient en fait 13 machines physiques. Aujourd'hui, 13 serveurs racine représentent plus de 1800 machines. Ainsi, Anycast nous a permis de faire évoluer le système dans une nouvelle dimension qui pourrait servir une communauté beaucoup plus large. Si vous êtes vraiment intéressé par un peu plus de l'histoire, le document RSSAC 023 a quelque chose d'intéressant à vous montrer.

Les identificateurs des serveurs racine et leurs opérateurs. Ces adresses sont toutes publiques. Nous fonctionnons tous sur des adresses IPv4 et IPv6, et nous le faisons depuis un certain temps. Il y a un site Web que vous pouvez consulter maintenant, root-servers.org, et il y a une jolie

petite carte que vous pouvez agrandir, la regarder et trouver l'emplacement de ces 1800 instances. Ce n'est pas nécessairement la même chose que l'endroit où ils sont situés topologiquement parce que l'Internet n'est pas exactement la même chose que la géographie, mais vous trouverez une distribution vraiment large de l'emplacement de ces serveurs. Vous n'avez pas besoin d'en avoir un physiquement près de vous parce que c'est l'Internet. Vous pouvez joindre n'importe lequel. Vous pouvez, à partir d'ici à Istanbul, parler à n'importe quel serveur racine et ils partageront ça. Il peut vous diriger vers un qui soit proche de vous. Il peut vous conduire à des milliers de kilomètres, mais vous allez obtenir une réponse.

Élaborer un ensemble de principes de fonctionnement de base dans le RSSAC. C'est probablement trop à lire. Je suis sûr que vous pouvez regarder ceci dans un diaporama en ligne. Je veux en appeler quelques-uns seulement. Ce sont toutes des choses qui nous tiennent à cœur, et nous rappelons le principe numéro deux selon lequel l'IANA est la source des données DNS de la racine. C'est donc de là que nous obtenons nos données, IANA via la zone racine — un Internet, une zone racine. Si vous demandez à l'un de ces 1800 serveurs sur Internet, ils regardent exactement la même base de données.

La diversité est une force du système global des serveurs racine. Nous avons donc la diversité du matériel, la diversité des logiciels, la diversité des organisations. Si une défaillance survient chez un fournisseur particulier de matériel, elle n'affectera pas l'ensemble du système. La même chose avec le logiciel. S'il y a un bogue dans un logiciel particulier, il n'affecterait qu'une petite partie du système global. La

même chose avec nos industries. Nous avons des agences gouvernementales, nous avons des organisations à but lucratif, des organisations à but non lucratif, des institutions éducatives. Ainsi, l'échec d'une industrie particulière ne va pas affecter les opérations du serveur racine. Les RSO, en tant qu'opérateurs de serveurs racine, collaborent et s'engagent beaucoup entre eux et avec la communauté des parties prenantes. C'est pour ça que nous sommes ici. Nous travaillons en étroite collaboration sur certains des problèmes technologiques au fur et à mesure que nous évoluons et maintenons le système des serveurs racine. Mais nous sommes aussi anonymes, autonomes et indépendants pour ne pas nous contrôler les uns les autres. Nous n'avons aucune autorité les uns sur les autres, mais nous faisons ce travail collectivement.

Quelques mythes sur le système des serveurs racine disent que nous avons un certain contrôle sur la destination du trafic Internet. Ce n'est certainement pas vrai. Les routeurs font ça. Nous fournissons une partie du processus de résolution de noms. Les requêtes sont gérées par un serveur racine. Nous avons vu dans la diapositive précédente ce résolveur récursif et cette mise en cache. Très peu de requêtes DNS aboutissent réellement à contacter le système des serveurs racine. Le contenu est contrôlé par l'IANA. Nous ne sommes que les opérateurs informatiques. Nous sommes juste le département informatique de la zone racine. Ils sont lettrés de A à M, mais il n'y a pas de signification spécifique à ces lettres. Elles sont simplement assignées au hasard. Sur la diapositive précédente, ce dernier mythe sur les instances de serveur racine qui reçoivent la requête DNS entière. Si vous demandez www.example.com, cette question entière nous arrive habituellement.

Nous voyons les résolveurs récursifs demander quelle est l'adresse de www.example.com. Nous savons que nous ne répondrons qu'à la question où est .com. Il y a en fait une technologie appelée minimisation QNAME qui permet au résolveur récursif de réduire cette requête de sorte que ce que nous voyons comme le système des serveurs racine ne correspond pas à l'adresse de www.example.com. Nous avons un peu plus de protection de la vie privée que votre résolveur récursif pourrait mettre en œuvre.

Quelques recommandations sur l'utilisation du système des serveurs racine. Si vous utilisez un résolveur récursif, vous pouvez par exemple vérifier les routes vers vos instances. Ainsi, vous pouvez tracer un itinéraire ou quelque chose d'autre pour savoir où se trouve chacune des instances. Et en général, il y a trois ou quatre qui sont proches. Nous n'avons pas de définition précise de proximité. Il s'agit généralement de mesures ou de latence. Nous vous recommandons d'utiliser un résolveur validant des DNSSEC au cas où quelqu'un d'autre serait [inaudible] vous avez la possibilité de vérifier que cette information est correcte. Nous vous recommandons de participer aux communautés techniques du DNS. Le RSSAC a un nombre assez limité d'opérateurs de serveurs racine, mais nous avons aussi un Caucus RSSAC, qui est ouvert aux experts DNS. Beaucoup de notre travail au RSSAC, se fait dans ce Caucus. Si vous souhaitez y participer, vous pouvez consulter le site et chercher le Caucus. Il y a des informations sur la façon de demander l'adhésion. Certains opérateurs de serveur racine demanderont en fait la possibilité d'héberger une instance de leur serveur racine dans votre réseau quelque part. Donc, la façon de le faire est de parler à l'un des membres du RSSAC ici ou aux opérateurs de serveur racine ici et

d'envoyer un courriel à ask-RSSAC@ICANN.org. Cela nous arrivera aussi. Jetez un coup d'œil à ça. [inaudible] beaucoup de statistiques sur l'utilisation du système des serveurs racine. Il s'agit donc d'examiner les requêtes dans leur ensemble, essentiellement une moyenne des requêtes par jour. Et nous parlons d'environ 100 milliards de requêtes par jour que nous voyons collectivement. Cela semble être beaucoup. La plupart d'entre elles sont des déchets et des choses mal configurées, mais il est certain que nous voyons un surapprovisionnement. Il y a beaucoup de capacité là. Très bien, cela dit, je vais le remettre la parole à Liman pour parler d'Anycast.

LARS-JOHAN LIMAN : Bonjour, je m'appelle Lars Liman. Je travaille pour Netnod, qui exploite un ensemble de serveurs racine. Et je vais essayer de parler un peu d'Anycast. Alors, Anycast n'est en fait pas directement lié au DNS. C'est une astuce du réseau que nous utilisons pour pouvoir partager la charge entre plusieurs serveurs pour chaque opérateur de système racine. Tous ces 1800 serveurs que Ken a mentionnés, ils sont regroupés dans des groupes de tailles différentes entre les différents opérateurs. Netnod exploite environ 75 ou 80, sur ce total de 1800 nœuds. Et tous les serveurs exploités par le même opérateur, par les mêmes adresses IP. Il en a deux, un pour IPv4 et un pour IPv6. Normalement, vous ne pouvez pas avoir deux ordinateurs sur le réseau avec la même adresse IP. Mais Anycast est une astuce qui vous permet de le faire de la même manière que nous avons des copies identiques.

Je vais faire une analogie ici. Si vous voyagez en Europe avec votre téléphone portable, vous pouvez composer... S'il vous arrive de vous

retrouver dans une situation d'urgence où vous avez besoin d'une ambulance, vous pouvez composer le 112 à partir de votre téléphone. Et vous arriverez à un centre d'intervention d'urgence qui vous aidera à faire envoyer une ambulance là où vous êtes. Si vous êtes à Amsterdam, aux Pays-Bas, et composez le 112, vous atteindrez un centre d'intervention d'urgence près d'Amsterdam. Mais si vous voyagez à Rome en Italie et composez le 112, votre appel téléphonique n'ira pas à Amsterdam. Il ira à un centre d'expédition à Rome ou à proximité de Rome. Et c'est la même astuce que nous utilisons, mais en termes d'Internet. Donc, si votre résolveur, l'ordinateur qui vous aide à vos recherches sur Internet, si votre résolveur est situé à Amsterdam et essaie d'atteindre un serveur de noms racine sur une certaine adresse IP, il atteindra un serveur de noms racine à Amsterdam ou près d'Amsterdam. Si votre serveur est situé à Rome en utilisant la même adresse IP, il atteindra un serveur à Rome ou près de Rome. Et ce ne sont que deux exemples. Maintenant, nous avons des serveurs dans 75 emplacements et les autres opérateurs ont peut-être dans 50 ou 200 emplacements également dans le monde entier. Et parfois, nous les avons au même endroit et la plupart du temps, nous les avons dans des endroits différents. Il y a donc tout ce réseau de serveurs et il y en a toujours un près de vous. Ainsi, en utilisant ces numéros spécifiques pour atteindre le serveur racine, vous pouvez toujours atteindre un à proximité.

Je vais donc essayer d'illustrer cela avec quelques diapositives. Mais avant ce faire, je soulignerai également que cela nous donne quelques caractéristiques intéressantes. Non, je vais d'abord passer en revue les diapositives en fait. La diapositive suivante s'il vous plaît. Merci. Sur

Internet, les paquets Internet essaient de prendre le chemin le plus court entre deux ordinateurs. Et typiquement, il faudra passer par un certain nombre de routeurs ou je vais ... J'utilise légèrement à tort le terme commutateurs de réseau qui transfère le trafic entre les différents liens et essaie ensuite de transférer le paquet de plus en plus près de la destination. Et dans le cas normal où vous n'utilisez pas Anycast, vous allez entre deux adresses IP uniques. L'adresse de l'expéditeur et l'adresse du destinataire et vous vous dirigez vers l'adresse du destinataire. Tous les routeurs vont donc travailler ensemble pour envoyer vos paquets vers la fin, la destination, le serveur que vous voulez atteindre. Et les requêtes DNS sur le Net sont du trafic Internet normal. Il n'y a rien de spécial avec les paquets DNS. Ils suivent donc le même principe. Si vous envoyez la requête DNS du résolveur à gauche à un serveur DNS à droite, elle passera par le réseau. Diapo suivante, s'il vous plaît.

Imaginez maintenant que vous avez trois destinations identiques. Ça fonctionne en fait de la même manière. Elles ont la même adresse IP. Elles ont le même contenu de base de données. C'est très important. Et elles utilisent le même réseau, de la même manière pour se connecter au réseau. Le paquet de la source tentera d'atteindre le plus proche. Et cela fonctionne en fait par les destinations qui disent au réseau, me voici, me voici, voici mon adresse IP. Et vous irez à la plus proche que vous écouterez et entendrez comme la voix la plus forte, pour ainsi dire. Une bonne chose avec ceci est que différentes sources finiront à différents endroits. Diapo suivante s'il vous plaît.

Donc, la source verte à gauche atteindra le serveur en bas à gauche parce que c'est le plus proche de cette source. Mais la source rouge en haut à droite atteindra le serveur en haut à droite parce que c'est le plus proche de cette source. Donc, selon l'endroit où vous vous trouvez sur le réseau, vous irez toujours à la destination la plus proche pour vos requêtes DNS ou cela peut être également utilisé dans d'autres contextes. Il ne doit pas s'agir uniquement du DNS. Bien sûr, il est très important que ces destinations bleues soient synchronisées. Ainsi, peu importe où va votre requête, la réponse est la même. Et c'est le travail des opérateurs de serveur racine de s'assurer que tout soit bien synchronisé et que les données soient modernes et correctes.

Cela a beaucoup de fonctionnalités intéressantes auxquelles vous ne pensez pas immédiatement. La première est que si vous avez des attaques de déni de service distribué, quand vous avez de grands, grands, grands systèmes de petits ordinateurs éventuellement, ce pourrait être votre webcam à la maison, ce pourrait être votre ordinateur portable ou votre décodeur TV connecté à Internet et puis peut-être infecté par un virus qui enverra le trafic d'attaque vers une certaine destination. Si vous utilisez Unicast, l'ancien modèle, tout ce trafic ira à la même destination, car il n'y a qu'une seule destination. Et cela signifie que vous focalisez tout ce trafic d'attaque vers une cible donnée et que cette cible sera surchargée et ne pourra pas répondre correctement aux requêtes. Si vous utilisez Unicast avec ce modèle, les décodeurs dans la zone rouge atteindront la destination rouge, la destination en haut à droite, tandis que les caméras de télévision en bas à gauche frapperont le serveur en bas à gauche. Vous répartissez donc le trafic entre tous ces nœuds. Et si vous avez 1800 nœuds à attaquer,

vous devez avoir un assez grand réseau de caméras Web et configurer des boîtes et des ordinateurs portables pour attaquer cela, pour les surcharger tous. Et ce n'est que lorsque vous surchargez l'ensemble du système qu'il cesse de fonctionner. Donc, cette façon de passer massivement à des milliers de serveurs nous donne une bonne résilience pour ce type d'attaque.

Une autre caractéristique que vous ne réalisez pas immédiatement est que si nous devions supprimer le serveur en haut à droite et le supprimer entièrement du réseau, les routeurs intermédiaires en seront avertis. Il n'y a plus de serveur en haut à droite. Ainsi, le trafic sera ensuite transféré au nœud le plus proche suivant, qui est en bas à droite. Et cela se produit automatiquement lorsque vous arrêtez votre protocole de passerelle frontière, vos annonces BGP, disant que ce nœud n'est plus là, automatiquement tout le réseau de routeurs commutera et dira, oh, nous devons plutôt emprunter cette voie, puis aller par là. Et cela continuera à fonctionner de manière transparente. Bien sûr, le serveur en bas à droite recevra un volume de trafic un peu plus élevé, mais ce n'est pas un problème, car ils sont tous massivement surapprovisionnés. Chaque serveur est dimensionné multiplié par le trafic qu'il reçoit déjà dans un cas normal. Ce n'est donc pas un problème. Et la fonctionnalité ici est qu'en tant qu'opérateur de serveur racine, je peux mettre notre nœud à Londres, en Angleterre, hors service, mais vous ne le remarquerez pas. Tout va continuer à fonctionner très bien, et nous pouvons faire de la maintenance. Nous pouvons installer un nouveau système d'exploitation, ou changer un disque dur cassé, ou nous pouvons faire quoi que ce soit avec notre ordinateur, et puis nous le rallumons quand tout fonctionne. Oh,

maintenant le nœud est de retour ici. Il y a un chemin plus court et le trafic va commencer à retourner vers le serveur qui est réactivé. Cela nous donne donc beaucoup de flexibilité dans la maintenance de ces serveurs. Si vous remontez à 25 ans en arrière, alors qu'il n'y avait que 13 machines, si nous devions arrêter notre machine unique, cela a réduit un peu la résilience du système des serveurs racine dans son ensemble, et il pourrait être noté si vous le cherchiez attentivement, mais aujourd'hui, c'est tellement plus flexible et tellement plus facile à faire. Vous n'avez même pas besoin de vous dire que nous faisons de la maintenance, car elle se retrouve automatiquement dans le système de routage et continue à fonctionner. Je vais passer la parole à Wes pour parler un peu du Comité consultatif du système de serveurs racines et de son Caucus. Merci.

WES HARDAKER : Merci beaucoup, Liman. Je m'appelle Wes Hardaker. Je suis l'opérateur du serveur racine de l'Institut des sciences de l'information de l'Université de Californie du Sud, et j'ai d'autres rôles dont je vais vous parler dans une minute dans la diapositive appropriée, mais nous allons maintenant parler de ce qu'est le RSSAC et du Caucus RSSAC. On va laisser de côté les questions techniques pour passer au côté administratif.

Alors, qu'est-ce que le RSSAC? Son but est de conseiller la communauté et le Conseil d'administration de l'ICANN sur les questions liées au fonctionnement, à l'administration, à la sécurité et à l'intégrité du système des serveurs racine d'Internet. C'est très soigneusement formulé, et si vous le regardez, c'est une portée très étroite. Nous ne

conseillons pas sur le DNS. Nous ne donnons aucun conseil sur quoi que ce soit d'autre lié à l'ICANN. Nous ne donnons que des conseils liés au système des serveurs racine, et c'est tout. Ni l'IANA, ni aucune des autres parties de l'ICANN.

Alors, compte tenu de cela, que fait et ne fait pas le RSSAC ? Premièrement, nous nous engageons à fournir des conseils, comme je viens de le dire, principalement au Conseil d'administration. Presque tous nos conseils sont en quelque sorte dirigés vers le Conseil d'administration, mais généralement nous pouvons fournir des conseils à la communauté. Nous avons des documents qui suggèrent que la communauté se penche sur la recherche ou les études de suivi, par exemple. Les opérateurs de serveur racine sont représentés à l'intérieur du RSSAC, mais le RSSAC ne fait rien d'opérationnel. En fait, nous ne discutons pas de la façon dont tout ce qui, comme Liman vient de le décrire, était lié à Anycast ou à la façon dont nous hébergeons nos services. Cela ne fait pas partie du RSSAC. Le RSSAC n'est en fait que la partie politique du système des serveurs racine.

Nos dirigeants sont les suivants : Jeff Osborn, président du RSSAC et qui assis en face de moi, et Ken Renard, vice-président du RSSAC, dont vous avez déjà entendu parler. Et l'organisation elle-même est composée d'un représentant principal de chaque opérateur de serveur racine, d'un représentant et d'un représentant suppléant. Donc, comme Ken l'a mentionné plus tôt, il y a 13 opérateurs de serveur racine ou 12 organisations d'opérateurs de serveur racine, ce qui signifie qu'il y a, au total, 24 représentants des RSO au RSSAC. Et puis il y a des agents de

liaison entrants d'autres organes. J'en parlerai davantage sur la diapositive suivante.

Et puis le Caucus du RSSAC, que je vais décrire en détail, je pense que Liman en a déjà parlé un peu, ou c'est Ken qui l'a fait, excusez-moi. Mais c'est un corps bénévole d'experts techniques, et c'est là que nous faisons la plupart de notre travail. Le RSSAC lui-même n'est pas l'auteur de beaucoup de documents ces jours-ci. Nous avons transféré la quasi-totalité pour que plus de gens nous aident. J'y reviendrai dans une minute. Et les membres du Caucus RSSAC sont confirmés par le RSSAC sur la base de leurs manifestations d'intérêt. Ils soumettent donc également des manifestations d'intérêt [inaudible] sur une diapositive ultérieure.

Nous avons donc des relations de liaison avec un certain nombre d'autres organisations. Nous avons des agents de liaison entrants, des gens qui nous aident à l'intérieur du RSSAC. L'un provient de l'opérateur des fonctions IANA, la PTI. L'un d'eux vient du responsable de la maintenance de la zone racine, Verisign, qui est également, bien sûr, un opérateur de serveur racine lui-même. Ils ont donc deux rôles au sein du RSSAC. Nous avons un agent de liaison auprès du Conseil d'architecture de l'Internet de l'IETF. Et nous avons un agent de liaison auprès du Comité consultatif sur la sécurité et la stabilité, ou SSAC. Nous avons aussi des agents de liaison sortants. Il y a un agent de liaison sortant auprès du Conseil d'administration de l'ICANN. J'occupe actuellement ce rôle. Et je siège au Conseil d'administration de l'ICANN ; il y a des agents de liaison sortants auprès du Comité de nomination de l'ICANN, du Comité permanent de clients et du Comité de révision de

l'évolution de la zone racine. Le dernier est le RZERC, un autre comité consacré à examiner comment les changements au système de serveur de route pourraient fonctionner. Il est différent du RSSAC, qui s'occupe plutôt de la façon dont le système fonctionne. Le RZERC est responsable de la façon dont les changements pourraient se produire si nous devions apporter des modifications techniques.

Alors, qu'est-ce que le Caucus RSSAC ? Je l'ai mentionné plus tôt. Il a plus de 100 membres en ce moment qui sont tous des experts en matière de DNS. Ce sont des gens qui comprennent bien la technologie. C'est vers eux que nous nous tournons lorsque nous voulons réfléchir en profondeur à la façon dont nous pouvons améliorer le DNS ou comment pouvons-nous l'étudier davantage le système des serveurs racine. Ils ont tous soumis des manifestations publiques d'intérêt qui indiquent leur expérience avec le DNS, pourquoi ils sont intéressés à participer au Caucus RSSAC, et quel est leur niveau d'expertise. Et surtout, ils obtiennent le crédit public pour chacun de leurs travaux individuels. Si vous regardez en bas dans tous nos documents du RSSAC, vous verrez une section d'auteurs qui regroupe en fait tous les membres du Caucus RSSAC qui ont contribué à leur élaboration. Vous constaterez que le nombre de personnes qui contribuent à un document particulier est souvent assez important parce que nous obtenons beaucoup d'aide et que nous accordons beaucoup d'importance à leurs opinions.

Comme je l'ai mentionné, le Caucus est un nombre d'experts DNS qui apportent une expérience diversifiée aux publications que nous produisons pour nous assurer que nous y réfléchissions pleinement et

profondément, par opposition à quelques auteurs ne seraient pas en mesure de fournir cette diversité. Nous assurons également la transparence sur qui fait le travail. Les efforts du Caucus sont généralement ouverts. Et c'est un véritable cadre pour faire les choses au sein du RSSAC.

Je vais maintenant parler de l'évolution de la gouvernance du système de serveurs racine. Ce n'est pas exactement le RSSAC, mais c'est le RSSAC qui l'a en quelque sorte commencé. Ce qui s'est passé, c'est que lorsque nous avons assigné le 12e opérateur des serveurs racine il y a longtemps, il y a plus de 20 ans, il n'y avait plus de procédure pour les ajouter ou les supprimer si nécessaire. Alors, comment changer qui fait cela ? En juin 2018, le RSSAC a décidé d'amorcer cet effort pour comprendre ce que nous allons faire pour l'avenir. Comment allons-nous résoudre ce problème ? Nous avons produit le document RSSAC 37, qui était une approche de la gouvernance du système des serveurs racine, y compris la possibilité d'ajouter et de supprimer des RSO au RSS. Nous avons également produit un tas de principes auxquels quelqu'un a déjà fait référence sur notre fonctionnement et l'éthique que nous fournissons au système des serveurs racine, des choses comme le fait de ne pas filtrer le trafic et de répondre à toutes les requêtes qui nous parviennent.

Après la publication de ce document, le Conseil d'administration de l'ICANN a agi en conséquence par le biais des directives, par le biais des recommandations du document RSSAC 38, l'organisation a été invitée à créer le groupe de travail sur la gouvernance du système des serveurs racine. C'est ce qui se passe maintenant. Il y aura cinq réunions plus

tard dans la semaine qui sont ouvertes si vous voulez, et dans ce cadre nous développons un modèle de gouvernance qui préserve les 11 principes directeurs que nous avons documentés dans le document RSSAC 37, y compris la diversité, la collaboration et l'indépendance, et il inclut des représentants non seulement des parties prenantes du système des serveurs racine, mais aussi d'autres entités que nous allons aborder dans une diapositive dans un instant. Et finalement, ce sera un document de l'ICANN qui ira également au processus de l'ICANN pour commentaires publics ; alors, une fois que nous aurons terminé de documenter les résultats du GWG, la communauté de l'ICANN aura également l'occasion de commenter les résultats de ce travail.

Les parties prenantes du système des serveurs racine, nous l'avons défini dans le document RSSAC 37, et c'est bien sûr toute la communauté de l'ICANN qui a un intérêt direct dans le système des serveurs racine, tout comme les opérateurs de serveur racine. Nous faisons la maintenance du service ; nous sommes donc clairement intéressés à nous assurer qu'il continue à fonctionner, comme le font l'IETF et le Conseil d'architecture de l'Internet, de sorte que le cours d'ingénierie Internet est l'endroit où les spécifications du DNS sont réellement maintenues, écrites et développées, où les changements se produisent. C'était la semaine dernière à Dublin. Il y a beaucoup de participants de l'IETF qui sont ici cette semaine, et ils ont clairement un intérêt direct dans le système des serveurs racine car ce sont eux qui maintiennent le DNS dans son ensemble. Dans le groupe de travail sur la gouvernance du système des serveurs racine, il y a un certain nombre de personnes différentes qui représentent différentes organisations ; il y a un membre de chaque opérateur de serveur racine, deux membres

du groupe des représentants des opérateurs de registre, deux membres de la ccNSO, et deux membres du Conseil d'architecture de l'Internet que j'ai mentionné il y a une minute, et ensuite il y a aussi quelques agents de liaison. Les cercles bleus à droite, les trois cercles bleus, sont les deux agents de liaison du Conseil d'administration de l'ICANN, un agent de liaison du responsable de la zone racine et un agent de liaison de l'IANA.

Cela dit, nous arrivons à la conclusion de cette présentation. Dans une minute, nous répondrons à vos questions ; voici quelques ressources pour vous. Pour plus d'informations sur le RSSAC lui-même, nous avons une page Web au sein de l'ICANN, et dans cette page Web, vous trouverez une foire aux questions qui a été conçue pour être facile à lire ; si vous voulez en savoir plus sur le système des serveurs racine, c'est en fait une bonne chose de simplement lire de haut en bas parce que cela répond à un grand nombre d'idées fausses courantes. Nous avons aussi une liste de courriel, ask-RSSAC@ICANN.org. Si vous avez des questions sur le système des serveurs racine ou si vous voulez en savoir plus sur les ressources ou si certaines personnes nous écrivent pour savoir comment déployer un système des serveurs racine près de leur pays ou région, nous vous dirigerons généralement vers la FAQ parce que c'est une des choses [inaudible] pour plus d'informations sur le Caucus, surtout si vous êtes intéressé à rejoindre le Caucus, nous avons une page Web et aussi une adresse de courriel RSSAC-membership@ICANN.org. Si vous êtes intéressé à devenir membre, nous vous demanderons une manifestation d'intérêt, qui sera ensuite transmise au comité des membres du Caucus du RSSAC pour révision. Comme je l'ai mentionné précédemment, nous recherchons

généralement des experts en matière de DNS ou un autre domaine d'expertise dont le Caucus pourrait bénéficier pour aider à produire nos documents. Avez-vous des questions? Parfois nos faisons une pause au milieu de la présentation, mais pas cette fois-ci. Des questions sur des questions techniques ou sur quoi que ce soit sur le côté administratif.

ULRICH WISSER : Il n'y a aucune question dans le module Q&R. Pour rappel, levez la main dans la salle Zoom ou écrivez vos questions dans le module Q&R. Je vais les lire. Et si vous êtes dans la salle, approchez-vous du micro et, d'accord, allez-y s'il vous plaît. Bonjour à tous.

OMAR SHURAN : Ma question est juste une question informative concernant Anycast. Est-ce la même chose que les serveurs racine gérés par l'ICANN, les IMRS, ou non ?

WES HARDEKER : Anycast est une technologie de routage générique et tous les opérateurs de serveur racine l'utilisent. Un résolveur me dirait quand même que je veux accéder à IMRS ou que je veux accéder au serveur ISI de l'USC et vous serez redirigé lorsque vous essaierez d'accéder à l'infrastructure de l'opérateur de serveur racine en fonction de l'endroit où vous vous trouvez. Donc pour les 12, il y avait des périodes où certains opérateurs de serveur racine l'utilisaient. Je vais être honnête, nous avons été les derniers à passer à l'utilisation de la technologie Anycast. Mon prédécesseur pensait qu'il serait peut-être préférable que

nous retardions l'utilisation pendant très longtemps pour nous assurer que c'était un mécanisme stable et, maintenant, nous le savons. Le système de serveur racine n'est pas le seul à l'utiliser.

ULRICH WISSER : Eh bien, il n'y a pas de questions dans le module Q&R. D'autres questions dans la salle ?

WARREN KAMURI : Pourquoi les opérateurs de serveur racine font-ils ce qu'ils font ? Je veux dire, on dirait qu'il y a un coût non négligeable. Pourquoi dépensez-vous votre argent et votre temps à faire ça ?

WES HARDEKER : C'est une excellente question, Warren, qui se trouve au Caucus RSSAC et qui connaît la réponse. Mais nous apprécions la question. La réalité est que nous le faisons depuis longtemps et nous le faisons entièrement pour le bénéfice d'Internet, point final. Ce n'est pas bon marché. Nous ne sommes pas payés pour ce travail. Mon organisation a des batailles budgétaires chaque année pour savoir combien nous pouvons consacrer à l'achat de nouvelles infrastructures et à des choses du genre. Ce n'est pas un processus bon marché. Alors, Liman ?

LARS-JOHAN LIMAN : Je pourrais compléter la réponse. Cela remonte à l'époque où l'Internet était tout à fait différent. Aujourd'hui, l'Internet est un vecteur d'activités et de trafic important. Mais quand le DNS a été inventé et

quand le besoin de serveurs racine est apparu, quand le DNS a été inventé, nous avons commencé à avoir besoin de serveurs racine qui pourraient servir le premier niveau du DNS, très réduit. Et j'admets, comme Wes l'a dit, que lorsque l'opérateur de serveur racine de Netnod a été lancé, pas par Netnod parce que c'est une suite du premier, à l'Institut royal de technologie de Stockholm, c'était un poste de travail, un ordinateur de cette taille, et quelqu'un assis au bureau. C'était vraiment sans importance à l'époque. Nos systèmes d'aujourd'hui sont complètement différents. La maintenance est absolument professionnelle. Nous avons des dizaines d'employés qui s'occupent de ces questions ; il y a eu un développement de plus de 30 ans dans ce domaine que nous avons poursuivi progressivement. Mais au début, ce n'était qu'une simple question de l'IANA, pouvez-vous le faire pour nous? Bien sûr. Et nous avons compris que cela continue d'être un service très important pour la communauté Internet que nous voulons fournir.

Un avantage, si nous revenons à la partie de la présentation de Ken, c'est que nous avons des organisations très diverses. Comme vous l'avez mentionné Ken, nous avons des organismes gouvernementaux, des organismes à but lucratif, sans but lucratif, nous avons des institutions du secteur académique. Nous avons tous des bases financières différentes pour la façon dont nous opérons cette activité. Netnod trouve donc de l'argent pour fournir ce service à notre façon, alors que l'Université de Californie du Sud a une autre façon [inaudible] agence a une troisième façon et l'entité commerciale a une quatrième façon. Alors, même si les systèmes financiers devaient changer de manière significative, tous les opérateurs de services racine ne seraient

pas immédiatement touchés par le même changement. C'est donc aussi un type de diversité qui est très important pour la longévité, pour maintenir ce service sur une longue période. Merci.

WES HARDEKER : D'autres questions ?

KEN RENARD : Je ressens juste le besoin d'ajouter une autre réponse à celle qui a déjà été présentée parce que Wes travaille avec l'université, je suis le président d'une société à but non lucratif et on est arrivés au point où, sur Internet, quand vous dites que vous faites quelque chose gratuitement, les gens vont me jeter ça à la figure et dire que Facebook ne me facture pas non plus. Je veux que ce soit vraiment, vraiment clair. Mon organisation écrit des logiciels dont l'Internet a besoin pour fonctionner et nous les donnons. Toutes nos dépenses sont payées par des gens qui reviennent et disent : « J'ai besoin d'aide, puis-je acheter des services de soutien auprès de vous pour aider avec le logiciel libre pour lequel je ne vous ai pas payé ? Nous avons un million et demi d'utilisateurs de notre logiciel BIND dans le monde entier. Environ 100 d'entre eux nous versent de l'argent pour l'aide. En outre, nous prélevons environ 20 % de l'argent que nous gagnons en soutenant BIND et d'autres logiciels open source et nous le dépensons pour exploiter un système des serveurs racine. Donc quand nous disons que nous ne facturons pas pour ça, je ne veux pas dire que nous gagnons de l'argent en vendant toutes vos informations privées. Il n'y a pas d'échange d'informations privées. Il n'y a pas d'échange

d'informations. Il n'y a pas d'échange de contenus. Tout ce que nous faisons est simplement distribuer l'adresse d'un serveur faisant autorité qui sait où se trouvent les TLD. Quand nous disons que nous sommes un organisme à but non lucratif, que nous ne gagnons pas d'argent, c'est la déclaration la plus vraie que vous n'entendrez jamais. Il s'agit d'un véritable organisme à but non lucratif, qui ne fait vraiment pas d'argent. Nous faisons littéralement ça et si vous êtes cynique, peut-être que vous ne voulez pas l'entendre. Nous le faisons littéralement parce que j'exploite une entreprise de 19 personnes de 19 pays différents qui croient tous sincèrement qu'une seule source de noms Internet est assez précieuse pour aller gagner moins d'argent en travaillant pour un organisme à but non lucratif. Nous sommes vraiment engagés dans notre mission.

HANS PETTER HOLEN : S'il n'y a plus de questions, je peux vous donner une autre réponse parce que puisque nous sommes 12 opérateurs, nous avons tous des réponses différentes, n'est-ce pas? J'exploite la racine K, ou mon organisation le fait. On ne me laisse plus jouer avec le service. Nous sommes une organisation d'adhésion. J'ai environ 20 000 membres qui paient pour le fonctionnement de la racine K ainsi que d'autres services. Si vous vous demandez ce que ça coûte, vous pouvez consulter nos rapports financiers annuels ou notre plan d'activités et notre budget pour voir combien ça coûte. Si vous le divisez par le nombre de membres, vous pourrez dire qu'ils contribuent à hauteur de 50 euros chacun par an pour cela. Il y a beaucoup de façons différentes de financer ce travail, ce qui est une force du système et nous avons tous

des façons différentes. Il serait très étrange que tout le monde tombe dans une crise financière en même temps.

ULRICH WISSER : Eh bien, nous avons une question dans le module Q&R. Comment est la relation du RSSAC avec d'autres groupes et surtout les non-commerciaux ?

WES HARDEKER : Le RSSAC organise des réunions avec d'autres unités constitutives qui ont une sorte de liens directs avec nous ou le besoin direct de nous parler parce que, comme Ken l'a souligné plus tôt, nous servons la racine de l'IANA, n'est-ce pas ? Nous avons promis que la source des données que nous obtenons provient de l'IANA. La plupart des unités constitutives de l'ICANN qui représentent les TLD, par exemple, qu'il s'agisse de la ccNSO ou de la GNSO, communiquent directement avec l'ICANN pour obtenir le changement de fonctionnalité de ces TLD. Nous communiquons avec l'IANA. C'est notre objectif principal pour être réellement opérationnels. Nous avons des réunions régulières avec le comité consultatif sur la sécurité et la stabilité. Nous nous réunissons régulièrement avec le Conseil d'administration de l'ICANN. Nous nous réunissons avec l'ASO cette semaine. Nous nous réunissons donc au besoin. Et nous avons eu des réunions, je pense, avec ALAC récemment et dans le passé aussi. Nous nous sommes réunis avec le GAC ce matin. C'est donc au besoin. En général, nous n'aimons pas tenir des réunions à moins que ce soit vraiment nécessaire. Cette fois-ci, on ne se réunira pas avec le Conseil d'administration de l'ICANN. Nous l'avons fait

pendant les trois ou quatre dernières réunions. Il n'y a pas de besoin immédiat direct entre deux organisations. Nous ne faisons pas perdre le temps des gens en les faisant s'asseoir dans une réunion sans contenu.

LARS-JOHAN LIMAN : Mais je tiens à souligner que l'interaction est toujours la bienvenue. Il y a des problèmes qui, selon vous, impliquent les racines des opérateurs. Venez nous en parler, s'il vous plaît. Et si cela conduit à la nécessité d'avoir une réunion, nous sommes tout à fait ouverts à l'organiser. Mais on ne se réunit pas régulièrement à moins qu'il y ait des questions à discuter. Comme Wes l'a dit, il y a suffisamment de réunions dans ce contexte. Nous n'avons pas besoin de les ajouter juste pour le plaisir de se réunir. Mais nous nous réjouissons vraiment de l'interaction avec d'autres groupes et avec des individus. Si vous avez des questions concernant le système des serveurs racine, arrêtez-moi dans le couloir et demandez. Vous me trouverez. Je fais deux mètres de haut. Je suis facile à trouver.

KEN RENARD : Il y a 12 opérateurs de serveur racine, des organisations de serveur racine. Sept d'entre eux sont dans la salle en ce moment, donc nous pouvons lever la main. Nous sommes ici.

ULRICH WISSER : Eh bien, une autre question dans le module Q&R. Pouvez-vous m'en dire plus sur les opérateurs Anycast et quelle est la relation avec le RSSAC, le cas échéant ?

LARS-JOHAN LIMAN : Les opérateurs Anycast. C'est nous. Nous exploitons le réseau Anycast. Et attention, nous n'avons rien à faire de spécial avec les routeurs sur Internet. Alors. Dans le cas de Netnod, nous exploitons 75 serveurs dans différents endroits, et ce sont nos serveurs. Nous les exploitons. Nous les expédions pour allocation. Certaines personnes nous aident à les monter dans un rack et à les connecter avec les câbles nécessaires au réseau et à l'alimentation, etc. Mais ensuite, nous nous connectons au serveur et nous faisons l'opération ; le serveur annoncera dans la relation - nous devons négocier. Une relation, il annoncera au prochain routeur en amont vers le réseau. Il annoncera que maintenant le serveur racine de Netnod est ici avec cette adresse IP. Apportez-moi du trafic, s'il vous plaît. Il n'est donc pas nécessaire d'avoir un opérateur Anycast spécifique. Divers opérateurs de serveur racine exploitent leur propre sous-ensemble de ces 1800 serveurs. Et chacune de ces installations de serveur, il peut s'agir de plus d'une boîte physique. Il peut s'agir d'un couple de serveurs et d'un routeur local pour cet opérateur de serveur racine. Cette grappe, cette combinaison annoncera au routeur le plus proche que je suis ici. Envoyer le trafic vers moi. Et c'est tout ce dont on a besoin. Merci.

ULRICH WISSER : Existe-t-il des exigences légales ou techniques que les opérateurs de services racine doivent respecter quotidiennement, autres que le temps de disponibilité ?

HANS PETTER HOLEN : Nous avons tendance à dire que l'Internet n'est pas réglementé ou qu'il n'a pas de juridiction gouvernementale. Et c'est vrai pour les processus politiques de l'ICANN ou des RIR ou de n'importe qui d'autre. Mais chacun des opérateurs a une entité juridique dans un pays donné et est soumis aux lois de ce pays. RIPE NCC est en Europe et nous devons respecter la législation européenne. Mes collègues ici sont aux États-Unis. Ils doivent respecter la législation américaine. Ces lois ne règlementent pas en détail la façon dont nous fonctionnons. Mais il y a une nouvelle législation à venir pour imposer de nouvelles exigences sur l'exploitation des infrastructures critiques. Et cela se produit à un rythme différent selon les pays. C'est donc une période passionnante.

LARS-JOHAN LIMAN : Je voudrais ajouter quelque chose parce qu'il y avait aussi une question sur les spécifications techniques. Et oui, il y a quelques spécifications techniques. Nous, par exemple, nous devons suivre le protocole DNS spécifié par l'IETF, le Groupe de travail de génie Internet dans une certaine norme technique. Et il y a aussi un document qui décrit les attentes quant à la façon dont les serveurs racine devraient répondre aux requêtes DNS entrantes. Et cela est publié par le Conseil d'architecture de l'Internet en coopération avec les opérateurs de serveur racine. Mais le Caucus RSSAC, comme nous en avons parlé, a

produit un document avec des attentes en matière de niveau de service, qui a été publié ou sera publié très bientôt. S'il n'a pas déjà été publié, il le sera très bientôt. Il y a un certain nombre d'attentes établies sur les racines des opérateurs auxquelles nous sommes censés répondre avec des limitations techniques, des temps de réponse. Et entre la publication de nouvelles données aux données est mise à jour aux nœuds terminaux et des choses du genre. Donc oui, il y a des attentes techniques.

WES HARDEKER : Je crois que vous faites référence au document RSSAC 047. Pour ajouter un peu plus d'information, je dirai que nous ne pouvons pas simplement surveiller si nos dispositifs fonctionnent ou non. Je crois que vous seriez impressionné par la façon de gérer n'importe quel réseau, qu'il s'agisse d'un serveur racine, d'un serveur DNS, d'un serveur de fichiers ou d'un serveur Web. Le nombre de graphiques que nous devons créer, et le nombre d'alertes que nous recherchons, il ne s'agit pas seulement de savoir si ça marche, si ça marche trop lentement, s'il est accablé par le trafic, voilà ce qui me réveille vraiment la nuit. Le disque manque-t-il d'espace ? Il y a beaucoup de petites choses qui entrent dans l'exécution de l'infrastructure, et vous devez savoir immédiatement quand quelque chose échoue. Quand il y a quelque chose de nouveau qui apparaît, que nous n'avions pas pensé à contrôler auparavant, la première chose que je fais, c'est écrire un nouvel élément à contrôler. À ce moment-là, un collègue très doué crée des graphiques très intéressants, et je les regarde toute la journée.

LARS-JOHAN LIMAN : Il y a aussi beaucoup d'expérience. J'ai mentionné que nous avons probablement 10 personnes qui opèrent ce système, et il y a un certain nombre d'opérateurs chez chaque opérateur de serveur racine. Il n'y a pas que les quelques personnes dans la salle ici, nous sommes ceux qui s'en occupent, donc encore une fois, je n'aborde que très rarement les détails techniques des serveurs racine. Mais l'expérience de l'opérateur de serveur racine chargé de la gestion des services DNS est probablement mesurée en siècles. Si vous mettez beaucoup d'expérience quant à la gestion du DNS, à regarder le contenu du DNS, les flux de trafic du DNS, le contenu des paquets, les procédures de mise à jour, la surveillance, l'ingénierie du trafic du réseau, tout cela fait partie de l'opération d'un serveur racine. Nous avons tous cette expertise dans nos organisations respectives, donc il n'y a pas que les quelques personnes autour de la table ici.

YUSUF : Je m'appelle Yusuf, je fréquente l'Université Marmara à Istanbul. Ma question est, comment comprenez-vous qu'il y a assez d'instances dans une région, par exemple à Istanbul, il y a sept instances. Comment savez-vous si c'est suffisant, à qui incombe la responsabilité de contrôler ça ?

HANS PETTER HOLEN : Bien que je ne puisse parler que pour l'un des opérateurs de serveur racine, la racine-K, RIPE NCC exploite également des réseaux de mesure mondiaux avec plus de 13 000 sondes de mesure. Et nous utilisons ce réseau de mesure et d'autres sources pour examiner la latence à partir

de l'endroit où les sondes sont dans les réseaux et voir que nous fournissons un bon service à tous les niveaux. Maintenant, cela peut être utilisé par tous les opérateurs de serveur racine, certains utilisent d'autres mesures afin de voir si le service qu'ils fournissent est bon. Si vous êtes particulièrement intéressé à cette question, RIPE NCC prend également des applications ouvertes pour les nœuds hébergés, afin que vous puissiez nous contacter pour en obtenir un sur votre FSI local, par exemple. Si vous croyez qu'il devrait y avoir plus de distribution, vous pouvez nous contacter et en discuter. Et les autres opérateurs de serveurs racine peuvent avoir d'autres façons de le faire, et cela fait partie de la beauté de la diversité. Nous n'avons pas une façon commune d'aborder cette question, nous avons 12 façons différentes l'aborder, de sorte que même si ma façon n'est pas bonne, quelqu'un d'autre peut faire mieux.

WES HARDEKER : Il faut noter qu'Internet fonctionnait très bien avant Anycast, et qu'il y avait 13 serveurs. Vous n'avez donc pas vraiment besoin d'un serveur près de chez vous, comme nous l'avons indiqué précédemment, la mise en cache rend le serveur DNS de votre FSI rapide. Ce n'est pas parce que vous avez un serveur racine près de chez vous, très, très peu de questions arrivent réellement à la racine, donc le besoin d'arriver à la racine n'est pas critique.

TAHIR : Bonjour, Tahir de l'Université technique d'Istanbul. Je voudrais poser une question : dans Anycast, nous avons des serveurs équivalents

distribués autour de nous. Mais qu'en est-il des données ou des informations dont ils disposent ? Avez-vous des problèmes de synchronisation ou à quelle fréquence devez-vous tout synchroniser ? Disposez-vous de procédures en ligne ou hors ligne pour ces éléments ?

KEN RENARD : Oui, tous ces serveurs doivent être synchronisés de manière approximative. La zone racine est mise à jour peut-être d'une à trois fois par jour. Nous mesurons et publions les mesures de la vitesse à laquelle cela arrive, peu importe, RSSAC 002. Donc, généralement, une zone racine est publiée, et puis elle est disponible sur toute l'infrastructure. Cela peut prendre quelques secondes pour tout envoyer. Mais cela varie si une instance se trouve dans un emplacement distant qui ne dispose pas d'une bonne connectivité, cela prendra un certain temps pour y arriver. Nous avons donc rarement des problèmes avec cette synchronisation. Ça arrive. Mais il y a des paramètres de protocole DNS qui disent que si votre version de cette zone est tellement ancienne, arrêtez de la servir. Nous voulons donc éviter la situation où les données sont tout simplement trop anciennes, surtout si les signatures DNS ne sont plus valides, car elles ont également une durée de validité.

WES HARDEKER : Il est intéressant de noter que pour chaque enregistrement dans la zone racine, vous êtes autorisé à mémoriser pendant deux jours avant de demander à nouveau. Gardez donc à l'esprit qu'en fait, tous les documents ont une validité de deux jours.

LARS-JOHAN LIMAN : Et encore une fois, Anycast joue ici parce que si nous, à travers les systèmes de contrôle, nous gardons un œil sur tous les systèmes et nous vérifions qu'un paramètre que nous vérifions est correctement mis à jour. Si nous remarquons qu'il n'est pas correctement mis à jour et que nous ne pouvons pas le réparer rapidement, nous le désactivons. Nous éteignons ce nœud et le trafic n'y arrivera plus. Il ira à un nœud différent, qui est mis à jour, et nous pouvons résoudre le problème pendant qu'il ment. Et puis on le rallume quand tout fonctionne. Encore une fois, Anycast fonctionne pour notre avantage et pour le vôtre.

JUNAID MIYAJI : Bonjour, je m'appelle Junaid Miyaji, et je viens du Bangladesh ; c'est la première fois que j'assiste en personne à une réunion de l'ICANN. J'ai une question à vous poser. Il y a quelques jours, nous avons été confrontés à un problème dans notre pays, à savoir l'arrêt de l'Internet. À ce moment-là, j'ai constaté que nous avons été déconnectés de tout l'Internet, mais que notre réseau IX fonctionnait bien. Pourtant, nous n'avons pas pu résoudre le DNS, car sans DNS connecté à l'Internet, il n'est pas possible de résoudre aucun nom de domaine. Avez-vous des options pour faire fonctionner la zone racine avec les réseaux IX, je veux dire, l'Internet local, ou y a-t-il un autre moyen, comme un individu comme moi peut mettre en cache les enregistrements de la zone racine, pour nos pays en particulier ? Merci.

LARS-JOHAN LIMAN : Oui, oui, et oui. Donc, pour résoudre un nom DNS normal, vous avez besoin non seulement d'un serveur racine, mais aussi des niveaux suivants descendants. Et puis il explose dans le nombre d'alternatives très rapidement, donc vous devez mettre en cache beaucoup de données. Cela dit, la zone racine est en fait une information publique, vous pouvez donc la télécharger. Je peux vous montrer comment faire ça plus tard. Il y a un document de l'IETF qui décrit comment faire fonctionner cette zone dans votre résolveur local. Vous exécutez une copie de cette zone racine à l'intérieur de votre résolveur, de sorte qu'il n'a jamais à communiquer avec un serveur de noms racine. Et puis vous comptez uniquement sur vous-même. Vous pouvez copier cette zone régulièrement et faire ce qu'on appelle un transfert de zone à partir de certains nœuds ouverts. Les opérateurs ont des nœuds qui vous permettront de copier cette zone automatiquement. Et si votre réseau est en panne, et que vous ne pouvez pas copier une nouvelle version, il continuera à utiliser l'ancienne version pendant, je crois, une semaine ou plus. Donc, oui, il y a des moyens de contourner ce problème. Je crois, cependant, que pendant ce black-out, les serveurs racines au Bangladesh ont peut-être encore fonctionné, mais le prochain saut vers le bas, peut être le serveur com ou le... Désolé, je ne me souviens pas du domaine de premier niveau pour Bangladesh. Mais, encore une fois, les étapes ci-dessous pourraient ne pas fonctionner, car les serveurs pourraient être en dehors du Bangladesh pour les niveaux suivants, et nous ne pouvons pas vous aider avec ça.

WES HARDEKER : Il y a en fait six serveurs racine au Bangladesh qui auraient dû rester en activité, très probablement.

JUNAID MIYAJI : Je suis désolé, mais malheureusement, j'ai tout essayé ; la façon dont vous avez mentionné pour faire des serveurs DNS moi-même et mettre en cache les enregistrements racine et les transformer en résolveur. Malheureusement, cela n'a pas fonctionné pour moi, et c'est pourquoi j'ai posé cette question. De plus, pendant l'arrêt, nous avons... J'ai essayé de trouver mille façons de le faire fonctionner avec Anycast, mais cela n'a pas fonctionné du tout. Et aussi, pour que les dossiers soient résolus comme vous l'avez mentionné, cela n'a pas fonctionné pour moi non plus. Je crois que j'ai peut-être commis des erreurs techniques ou quelque chose du genre. Y a-t-il un moyen pour être en mesure de connecter avec des techniciens ou des choses techniques pour régler ces problèmes en dehors de ...

WES HARDEKER : Il y a plusieurs choses auxquelles vous faites référence. Il y a donc deux parties, n'est-ce pas ? Imaginez que vous essayiez de chercher le nom d'un site Web, par exemple, et que ce site est en cours d'exécution et que je choisirai Antarctique, pas dans un pays, ok ? Si une région n'est pas sur Internet, c'est peut-être à cause d'une catastrophe naturelle comme un ouragan ou autre, que ce soit politique ou pas, il n'y a aucun moyen d'y arriver, ok ? Le serveur Web est en Antarctique, donc même si vous pouviez le consulter, ça ne marche pas, ok ? Maintenant, l'autre aspect est si le serveur DNS, disons que vous cherchez example.com, si

le serveur DNS pour example.com est en Antarctique et que vous êtes hors service pour une raison quelconque, une coupure de câble, peu importe. Votre FSI peut démarrer à la racine et vous l'obtiendrez parce qu'il est juste là, mais le serveur racine ne peut pas réparer votre accès en dehors d'un environnement. Le serveur racine n'est pas en mesure de corriger cela pour vous.

JUNAID MIYAJI : Merci, mais je suppose que j'ai raté un certain point. J'en suis conscient. Ce dont je parle c'est des réseaux IX ; nous avons quelques serveurs dans nos réseaux locaux, comme j'ai mes serveurs au Bangladesh, à Dhaka. Ils devraient donc être en mesure de résoudre les sites Web qui sont hébergés à Dhaka, pas en dehors du Bangladesh, mais je voudrais résoudre les noms de domaine qui sont hébergés au Bangladesh. Et ces sites en particulier travaillaient avec les réseaux IX, et nous étions en mesure de les résoudre directement par IP, mais pas avec les noms de domaine que nous pourrions résoudre en utilisant les zones racine. C'est ça ma question.

KARL REUSS : Nous travaillons en partenariat avec un centre d'échange de paquets PCH pour fournir un grand nombre de nos nœuds Anycast. Nous nous sommes associés avec eux et nous faisons fonctionner nos serveurs à partir de leur infrastructure. Ils aident de nombreux pays à mettre en place des points d'échange et à héberger leurs propres DNS internes pour leur domaine de premier niveau. C'est le type d'activité où vous avez besoin de beaucoup de choses pour être mis en place et

fonctionner correctement, et il est difficile de les tester à moins que tout soit cassé. Vous devez passer par de nombreux dépannages pour vous assurer que tout soit correctement configuré. Nous pouvons travailler avec vous. Je sais que nous sommes au Bangladesh. Nous pouvons analyser ce que vous avez fait et essayer de voir si nous pouvons identifier quelque chose qui ne soit pas configurée correctement. Il y a plusieurs pièces et le serveur racine est juste l'une d'entre elles. Le serveur racine peut bien fonctionner, mais il y a encore beaucoup de choses qui peuvent être erronées.

HANS PETTER HOLEN : Je voudrais ajouter quelque chose. Je pense qu'il s'agit d'un problème très intéressant que seuls quelques très rares pays ont effectivement testé à grande échelle. Comment pouvez-vous maintenir l'infrastructure du pays en fonctionnement si vous perdez la connectivité avec le reste du monde ? Certains pays l'ont testé et on soupçonne pourquoi ils le font. Certains disent que c'est pour mettre leur pays hors service. Certains disent que c'est pour se défendre. Ces tests en soi ont été considérés comme controversés. Je pense que nous, en tant que communauté des ingénieurs, nous devrions nous réunir, examiner la question et voir comment nous pouvons faire en sorte qu'un sous-ensemble du réseau fonctionne le plus possible en termes de crise. Parce que maintenant, dans le monde, il y a des pays qui ont des conflits armés en cours et il y a des catastrophes naturelles et autres. Tout ce que nous pouvons faire pour comprendre cela et nous assurer que l'Internet reste résilient, je pense que cela vaut la peine d'être abordé. Mais comme je l'ai dit, les serveurs racine sont une très

petite partie ici. Je pense que c'est plus pour ceux d'entre nous qui sont également engagés dans d'autres activités dans le DNS.

KARL REUSS : Il semble que nous avons beaucoup de services par PCH au Bangladesh. Il semble que beaucoup de pièces sont là comme elles devraient être et je pense qu'elles ne sont tout simplement pas complètement mises en place comme elles doivent l'être.

WES HARDEKER : Votre problème n'est malheureusement pas le serveur racine. C'est plus comme .bd ou certaines des autres infrastructures. Mais il faudrait une analyse pour y arriver. D'autres questions ?

ULRICH WISSER : Nous pensons que nous avons déjà dépassé le temps alloué. Merci à tous d'être venus.

[FIN DE LA TRANSCRIPTION]