SAN JUAN – Comment ça marche : les opérations du serveur racine
Lundi 12 mars 2018 – 10h30 à 12h00 AST
ICANN61 | San Juan, Porto Rico

CATHY PETERSEN : Bonjour à tous. Bienvenue à cette séance sur « Comment cela fonctionne ». Nous avons un peu de retard suite à cette cérémonie d'ouverture qui a été magnifique. Soyez patients, nous allons commencer sous peu. Merci.

ORATEUR NON-IDENTIFIÉ : Nous allons commencer dans deux, trois minutes. Nous avons pris 15 minutes de retard parce que la cérémonie d'ouverture a duré un peu plus. Mais nous allons vous prier d'être prêts à commencer dans deux, trois minutes. Merci.

CATHY PETERSEN : Bonjour à tous encore une fois. Soyez les bienvenus à cette séance de « Comment cela fonctionne ». Pour cette séance, nous allons aborder les opérations du serveur racine. Nous vous remercions encore une fois d'avoir été patients.

Andrew McConachie est le premier présentateur. Andrew, allez-y.

Remarque : Le présent document est le résultat de la transcription d'un fichier audio à un fichier de texte. Dans son ensemble, la transcription est fidèle au fichier audio. Toutefois, dans certains cas il est possible qu'elle soit incomplète ou qu'il y ait des inexactitudes dues à la qualité du fichier audio, parfois inaudible ; il faut noter également que des corrections grammaticales y ont été incorporées pour améliorer la qualité du texte ainsi que pour faciliter sa compréhension. Cette transcription doit être considérée comme un supplément du fichier mais pas comme registre faisant autorité.

ANDREW MCCONACHIE : Merci. Bonjour, je suis Andrew McConachie. Je travaille pour le soutien de politiques de l'ICANN. Je soutiens de le RSSAC et j'aborderai le système de serveur racine.

Nous allons commencer par un peu de contexte. Nous avons divisé ce programme en quatre parties : un aperçu du système de noms de domaine, le système de serveur racine actuel et ses fonctionnalités et puis je céderai la parole à Steve Sheng, ici à mes cotés, qui vous expliquera Anycast et puis abordera le RSSAC et certaines activités récentes du RSSAC. Par la suite, nous aurons une séance de questions et réponses avec certains des opérateurs de serveur racine qui sont dans la salle et nous allons leur demander de nous rejoindre à table pour répondre aux questions. Donc si vous avez des questions, gardez-les jusqu'à la fin.

Nous allons commencer donc par un aperçu du système de noms de domaine et des serveurs racine. Alors qu'est-ce que c'est que les adresses IP et comment fonctionnent-elles en tant qu'identificateurs sur internet ? Les adresses IP sont les identificateurs fondamentaux sur internet et tous les hôtes connectés à l'internet ont besoin d'avoir des adresses IP, que ce soit du type IPv4 ou IPv6, ou s'ils opèrent à travers un réseau, c'est toujours des adresses IP dont ils ont besoin, les adresses IP

étant donc des étiquettes numériques qui ne sont pas faciles à retenir ; ce sont des suites de numéros. Voilà. La zapette ne fonctionne pas très bien ce matin.

Alors pourquoi avons-nous besoin du DNS ? À l'origine, comme je l'ai dit tout à l'heure, les adresses IP n'étaient pas faciles à retenir et elles changeaient souvent. Donc le problème avec le DNS était qu'il nous fallait des noms que les personnes puissent retenir pour pouvoir se rappeler des adresses, pour pouvoir se rappeler comment accéder au site.

Ces problèmes existent toujours mais il y a d'autres problèmes modernes, comme par exemple le fait que les adresses IP peuvent être partagées et qu'il se pourrait qu'il y ait différentes adresses IP qui accèdent au même service. Donc le problème moderne est qu'on avait des points d'entrée ou d'accès multiple à ce site et vice versa.

Le système des noms de domaine est donc hiérarchique. Comme vous voyez sur le schéma à l'écran, nous avons au sommet la racine et au-dessous, nous avons les noms de domaine de premier niveau, connus également comme TLD dont certaines extensions comprennent le .edu, .mil, .uk. Au-dessous de ce niveau, nous avons une deuxième couche ou un deuxième niveau, puis un troisième niveau et ainsi de suite. Il s'agit donc d'une cartographie de noms à adresse IP. Mais il y a

également d'autres systèmes de repérage ou de mappage qu'on connaît, c'est-à-dire les serveurs de courrier que l'on connaît comme enregistrement PTR, des noms et puis le système inverse qui nous permet de revenir du chiffre au nom.

Ici, on voit un schéma un peu plus compliqué. Je vais prendre un moment pour vous expliquer ce diagramme, qui est censé montrer le processus de résolution du DNS, c'est-à-dire comment on utilise vos expériences avec le DNS, ce que doit ou par quoi l'utilisateur doit passer, c'est-à-dire le flux de fonctionnement du DNS pour que l'utilisateur puisse accéder d'un nom de domaine à une adresse IP, et finalement à un site web.

Ici à droite, on a un utilisateur internet qui est le client qui veut vraiment accéder au site www.example.com comme server web. Donc pour commencer, il va ouvrir un navigateur qui va lui demander de saisir un nom de DNS, qui passera alors par un serveur de noms récursif. Et on suppose que ce serveur de noms récursif n'a pas d'information en cache. Donc pour cette démonstration, on assumera que ce serveur vient d'être allumé, qu'il n'a pas d'informations, qu'il ne sait rien.

Donc qu'est-ce qu'il va faire ? On vient de lui donner une requête pour accéder au site www.example.com. Avant de rendre une réponse à l'utilisateur, il va commencer par accéder à la racine.

Donc il demandera à la racine : « Regardez, j'ai besoin d'accéder à cette adresse : www.example.com. » Et le serveur racine dira : « Aucune idée mais je sais où trouver le .com. » Donc la réponse du serveur de noms racine au serveur de noms récursif sera où trouver le .com.

Donc le serveur récursif contactera alors le serveur de noms du .com pour lui demander où trouver l'adresse example.com. Leur serveur du nom .com dira : « Aucune idée mais je sais où trouver le serveur du nom example.com. Le voilà. » Et donc le serveur de noms récursif accédera au serveur de nom example.com pour lui demander où trouver le www.example.com. Et finalement, le serveur de noms récursif obtiendra la bonne réponse et la fera passer à l'utilisateur internet avec l'adresse IP de ce nom de domaine qui est www.example.com.

Voilà comment un utilisateur passe par tous nos processus de résolution d'un nom de domaine vers une adresse IP pour accéder à une page web.

Or dans cette diapositive, on a également un autre aspect qui est l'aspect sécuritaire, que l'on connaît comme DNSSEC ou sécurité du DNS. C'est-à-dire que pour chacune de ces questions, pour les communications entre le serveur de noms récursif et chacun de ses serveurs de noms faisant autorité – que ce soit le serveur de racine ou du nom .com ou du nom

example.com – les réponses qui sont envoyées au serveur de noms récursif de ces serveurs faisant autorité sont signés, c'est-à-dire que le serveur récursif peut valider cette réponse est la bonne réponse, qu'il n'y a pas eu d'intervention entre les deux, qu'il n'y a pas d'autres serveurs de noms qui n'est pas le bon qui lui donne la réponse. Et c'est cela le DNSSEC, c'est ce qui permet de vérifier que c'est le serveur de noms faisant autorité qui a répondu. Donc voilà le processus de résolution de noms de domaine.

La zapette a besoin de quelques pousses... Bien. Donc comme on disait, le serveur de racine n'a besoin de savoir que ce que l'on va demander par la suite. On a une liste de serveurs comme .com ou .net et .org. Or en général, ce n'est pas la question qu'on leur demande souvent.

On avait une situation hypothétique où on venait d'allumer le serveur de noms récursif qui n'avait pas d'information en cache, ce qui est rare en réalité. Les serveurs récursifs ont beaucoup d'informations en cache en général et la plupart des requêtes qui sont envoyées au serveur de nom, en fait, sont déjà en cache, c'est-à-dire qu'il y a peu de requêtes envoyées à la racine ou moins que ce que l'on pourrait penser.

Il y a eu quelques modifications modernes au DNS. J'ai expliqué le DNSSEC, connu comme extension de sécurité ou sécurité du

DNS. Le DNSSEC vise à signer les réponses qui sont envoyées aux serveurs de noms récursif pour que ces derniers à la fois puissent valider ces réponses. Par valider, j'entends qu'en fait, on peut vérifier qu'il s'agit de la bonne réponse parce qu'on a une signature cryptographique qui valide la réponse et le fait que la réponse est correcte.

Il y a également des améliorations à la confidentialité. On y travaille toujours au sein de l'IETF, l'équipe de travail de génie internet. Donc par exemple, on travaille sur une couche de sécurité du transport des informations internet qui sécurisera la transmission de la requête pour garantir qu'il n'y ait que les deux parties appliquées à l'échange qui puissent voir ces informations.

Une autre modification moderne est le système Anycast. Le système Anycast travaille beaucoup avec les serveurs racine et en général permet que différents serveurs partagent une même adresse IP et protège les serveurs des attaques de déni de service, de DoS. Mon collègue Steve abordera cette question plus tard.

La zone racine vis-à-vis des serveurs racine, c'est-à-dire que la zone racine a les données qu'utilisent les serveurs racine, c'est-à-dire que la zone racine est le point de départ. C'est une liste de noms de TLD et de serveurs de noms. C'est un schéma qui est

donc géré par l'ICANN par politiques communautaires. Il s'agit d'une liste consolidée et distribuée par maintenant le responsable de l'entretien de la zone racine à tous les opérateurs des serveurs racine. Et en définitive, c'est la base de données avec tous les contenus qu'utilisent les serveurs racine.

Les serveurs racines répondent avec les données contenues dans la zone racine. En ce moment, on a 13 identités différentes qui composent entre toutes le serveur racine, qui sont distribuées sur 900 instances. Il s'agit d'un rôle purement technique. Et chacun des opérateurs de serveur racine, en fait, est responsable de sa propre exploitation.

On se demande ici ce que c'est qu'un opérateur de serveur racine. On a en ce moment 12 groupes de génies professionnels différents qui se centrent sur la fiabilité et la stabilité du service pour qu'il soit accessible à tous les utilisateurs internet. Ils coopèrent entre eux, ils sont professionnels. Il s'agit d'un groupe d'organisation divers, c'est-à-dire qu'il y a des organisations qui varient en termes géographique, organisationnel et technique.

Cependant, les opérateurs ne s'impliquent pas à l'élaboration de politiques et à la modification de données. Ils ne font qu'en fait desservir ces données. Pourtant, ils s'impliquent à l'évolution ou l'extension opérationnelle du service, à l'évaluation et au déploiement suggéré des modifications

techniques et des domaines [inintelligible] qui pourraient être élaborés par l'IETF. Et ils s'assurent que le service soit toujours stable, robuste et accessible à tous les utilisateurs de l'internet.

Donc voilà un peu le contexte sur le DNS. C'était un peu technique mais probablement pas trop. Nous allons maintenant entrer dans le domaine du système de serveur racine actuel et ses fonctionnalités. J'espère qu'on pourra passer la diapositive. Voilà.

Alors la croissance du système de serveur racine. Cette diapositive montre l'évolution historique de la quantité d'identités de serveurs racine au fil du temps depuis les années 80, donc vous voyez l'évolution. Et depuis 1998, nous avons 13 identités différentes. Ces changements répondent aux demandes techniques, aux questions d'extensibilité. Et à l'heure actuelle, les questions liées à l'extensibilité sont résolues par Anycast qui est un outil véritablement magnifique qu'utilisent les opérateurs de serveurs racine pour pouvoir aborder les questions liées à l'extensibilité.

Les serveurs de système racine exploitent leur service en IPv4 et en IPv6, c'est-à-dire qu'il y a 13 adresses IPv6 et IPv6 et il existe plus de 900 instances internationales, comme je le disais tout à l'heure.

Voici quelques uns des principes de base du système de serveur racine. Il y en a cinq. Il est important que le système du serveur racine fournisse une plateforme stable, fiable et résiliente pour le DNS, qu'il opère dans le bien commun de tout l'internet, que l'IANA est la source des données de racine du DNS c'est-à-dire les données qui sont dans la zone racine, que les changements à l'architecture sont fondés sur les résultats de l'évaluation technique et des besoins techniques tels que démontrés et que l'exploitation et les attentes techniques du DNS soient définies par l'IETF.

Si vous êtes intéressés par l'histoire du système de serveur racine, vous pouvez toujours télécharger et lire le document RSSAC023, l'histoire du système de serveur racine qui est disponible sur le site web du RSSAC.

On a ici une liste des opérateurs de serveur racine à l'heure actuelle. Vous voyez les 13 entités là-dessus, leur nom dot à gauche. Dans la colonne du milieu, vous voyez les adresses IP en IPv4 et IPv6, on a les deux versions pour chacun d'entre eux, chacun des hôtes. Et puis chacune des ces adresses IP en IPv4 et IPv6, au moins les adresses IPv4 en fait sont hébergées dans un nuage IPv4, c'est-à-dire que derrière ces adresses IP, il y a énormément de serveurs, ce qui arrive à plus de 900 en ce moment. Mais en fait, il y en a de plus en plus. La dernière fois que j'ai fait cette présentation, on en était à plus de 800 et

maintenant, on en est à plus de 900 donc vous voyez que cela évolue constamment.

Voici les serveurs racine dans l'actualité. Donc cette image a été tirée du site web root-servers.org. Cela vous montre où sont situés les serveurs racine. Ce n'est pas tout à fait exact, cela ne vous dit pas par exemple qu'il y a sept instances du serveur racine à Madagascar. Il s'agit d'un graphique. Mais si vous accédez au site web, il est possible de voir un peu plus de détails et voir les villes même où chaque instance se trouve. Ici, c'est un aperçu un peu général mais si vous accédez au site web, vous pourrez voir des informations bien plus détaillées.

Voilà la structure de gestion de la zone racine, c'est-à-dire que les données de la zone racine sont envoyées au système de racine, au système de serveur racine. Donc si on a besoin d'apporter un changement aux données hébergées dans la zone racine, quand vous changez vos enregistrements de colle ou certaines informations associées à vos registres, aux registres de votre TLD, vous allez contacter l'IANA pour faire ce changement qui sera alors communiqué aux mainteneurs de la zone racine, à l'heure actuelle donc Verisign. Et deux fois par jour, ce changement ou toute la zone en fait – non pas seulement les modifications – sera envoyée aux opérateurs de serveur racine. Et les opérateurs de serveur racine seront alors responsables de communiquer ces informations à tout le nuage Anycast et

d'envoyer ces informations à toutes les requêtes reçues des résolveurs de noms de domaine.

Certaines des fonctionnalités des opérateurs de serveur racine apparaissent ici à l'écran. Donc on a une diversité de structures organisationnelles, histoires opérationnelles qui varient également parfois. Ils utilisent différents matériels, différents logiciels, ils ont différentes plateformes de matériels et de logiciels, ce qui est utile au niveau de la sécurité parce qu'on a une corrélation forte entre les différents matériels et une sécurité consolidée. Et puis on a différents types de modèles fondationnels, c'est-à-dire qu'on a différents types d'organisations.

Ces opérateurs partagent leurs meilleures pratiques, ce qui leur permet d'avoir une sécurité de système physique améliorée, d'avoir une capacité qui a plus de fourniture que nécessaire et puis ils ont également du personnel professionnel à qui ils font confiance. Les opérateurs coopèrent à travers les différentes réunions de l'industrie et de la communauté, dont l'ICANN. Mais il existe également des réunions de l'équipe de travail de l'ingénierie internet, NANOG, RIPE, donc ce sont les réseaux régionaux. Il existe des groupes de recherche opérationnelle également mais ils utilisent en tout cas les outils de collaboration sur internet et ils ont des opérations qui sont toujours transparentes.

Les opérateurs collaborent également pour coordonner leurs réponses aux situations d'urgence pour pouvoir répondre à tout type de problèmes qui pourraient avoir lieu. Ils ont des activités périodiques qu'ils organisent pour pouvoir s'organiser pour pouvoir avoir des meilleures capacités de réponse en cas d'intervention en cas d'urgence. Et ils ont différents organismes internet établis.

À mesure l'internet évolue, il y a des nouvelles exigences que l'on applique au système du DNS. Les opérateurs donc par exemple ont adopté l'IPv6 comme réponse aux changements. On a également compris le DNSSEC et les IDN ici parce qu'il y a beaucoup d'IDN déjà hébergés dans la zone racine. Et le principal est de renforcer la capacité de réponse, la résilience et la force ou la solidité comme on dit de l'internet. Donc on a différentes instances d'Anycast, plus de 900.

On a [essayé] quelques mythes ou quelques fausses idées que l'on pourrait avoir par rapport au système de serveur racine. Mythe numéro 1, les serveurs de racine contrôlent tout le trafic internet, ce qui n'est pas tout à fait vrai. Ce n'est pas vrai du tout d'ailleurs, c'est un mythe. Ce sont en fait les routeurs qui vont contrôler par où passe le trafic internet. Peut-être que ce mythe existe parce que le DNS va mettre en vis-à-vis ou mettre en correspondance les adresses IP avec les noms de domaine mais

en général, c'est les routeurs qui vont contrôler pas où passent les paquets d'informations.

Un autre mythe est que la plupart des requêtes du DNS sont gérées par le serveur racine mais comme on a vu dans l'exemple, cela n'est vrai que si les informations étaient hébergées en cache dans le serveur de nom récursif ou que le serveur de noms récursif n'avait pas ces informations et qu'il devrait les demander. Mais en général, la plupart des requêtes du DNS ne sont pas gérées par le serveur racine. Dans la plupart des cas, il s'agit de requêtes qui sont gérées directement par le serveur de nom récursif.

La gestion de la zone racine, la fourniture des services, c'est la même chose – voilà le troisième mythe –, ce qui n'est pas vrai. On avait un diagramme qui montrait tout à l'heure la division des responsabilités et le changement de la manière dont ces informations arrivent à être divisées en requêtes.

Un autre mythe est que les identités des serveurs racine ont un sens spécial, ce qui n'est pas vrai, ou qu'il n'y a que 13 serveurs racine. On en a plus de 900.

Un autre mythe serait que les opérateurs de serveur racine exploitent leurs opérations de manière indépendante. Et bien qu'il s'agisse d'organisations indépendantes, ils travaillent en coordination, en collaboration entre eux, avec tous les autres

pour garantir que le service soit stable pour tout le système de serveur racine.

Et puis mythe final, les opérateurs de serveur racine ne reçoivent que la partie du TLD d'une requête, ce qui n'est pas tout à fait vrai. Ils vont recevoir toute la requête. C'est comme cela que fonctionne le DNS. Au sein de l'IETF, il y a des travaux en cours pour modifier cela. Si cela vous intéresse, le mot clé est QNAME minimization. Vous pouvez le consulter. À partir de cette initiative, chacun ne recevrait que la partie qui le concerne d'une requête.

Je vais maintenant céder la parole à mon collègue Steve Sheng qui présentera les deux parties qui reste, à commencer à Anycast.

STEVE SHENG : Merci Andrew. Je m'appelle Steve Sheng. J'appartiens au personnel de l'ICANN qui soutient le travail du RSSAC. Je vais vous parler d'Anycast et des activités du RSSAC.

Anycast est un système de routage... Excusez-moi, je vais revenir en arrière. Il y a deux termes ici : Unicast et Anycast. Et il y a une différence importante entre eux. Dans l'Unicast, les paquets ou les datagrammes venant des sources vont tous vers la même destination. Et une instance unique sert toutes les sources. En

cas d'attaque par déni de service des DoS, tout le trafic va vers une instance unique. Voilà pour Unicast.

Pour ce qui est de Anycast, il y a des instances multiples qui servent les mêmes données pour toutes les sources. Et donc ces instances ont toutes la même adresse IP. Et les routages intermédiaires déterminent donc la destination en fonction de la source. Cela veut dire que la source obtient les données plus rapidement et les attaques par déni de service sont envoyées à l'instance la plus proche. Je vais vous illustrer tout cela avec un diagramme, un schéma.

Ici, vous voyez une illustration d'Unicast. Vous voyez une source et une destination. La destination, c'est une instance unique et le trafic prend la route la plus courte vers la destination unique.

Dans le cas d'Anycast, vous voyez les trois destinations en bleu. Ces destinations ont toutes la même adresse IP. Et la politique de routage détermine quelle en est la plus proche, c'est-à-dire quelle est la destination la plus proche de la source. Et donc le trafic ou la route entre la source et la destination est plus courte.

Et quel est le rapport entre cela et les attaques par déni de service ? Dans ce type d'attaque, l'attaquant attaque la destination mais le trafic va uniquement vers la destination la plus proche. Alors l'une des destinations va être débordée mais les autres destinations peuvent encore recevoir du trafic.

Une des questions que l'on reçoit dans ce type de séance est de savoir de la part des opérateurs de serveur racine ainsi que des opérateurs de service... Si vous êtes un opérateur de réseau et que vous voulez avoir trois ou quatre instances, vous aurez une instance qui sera plus proche de vous et dans ce cas-là, le routage sera plus court. Mais vous allez vouloir également améliorer les routages. Vous pouvez avoir une instance proche de vous mais le trafic va quand même faire des tours. Et donc il est important de pouvoir tenir cela en compte.

Si vous êtes un opérateur de résolveur récursif pour augmenter votre cache, vous pouvez considérer le fait de déployer la technologie qui fait une copie de la zone racine et des adresses IP. Et le bénéfice de cela, c'est que parfois, cela réduit les risques liés à la confidentialité des serveurs récursifs aux serveurs qui doivent recevoir les requêtes. Il est important donc de mettre en place la validation DNSSEC qui va nous assurer que vous recevez des informations valides, que ces informations n'ont pas été modifiées.

Et finalement, nous invitons les experts techniques à participer et à contribuer au caucus RSSAC où des avis en matière technique sont élaborés.

Maintenant, je vais vous parler un petit peu, je vais vous donner un aperçu du travail du RSSAC. RSSAC veut dire comité

consultatif du système de serveur racine. Il a pour mission de conseiller la communauté de l'ICANN et le Conseil d'Administration par rapport à des questions liées au fonctionnement, à l'administration, à la sécurité et l'intégrité du système de serveur racine de l'internet. C'est un mandat très précis qu'a ce comité consultatif.

Une précision importante que je dois apporter car parfois, cela n'est pas bien compris au niveau de l'ICANN, c'est que le RSSAC est un comité qui produit des avis, en premier lieu vers le Conseil d'Administration mais aussi vers d'autres organes et organisations de l'ICANN qui participent à la gestion du DNS.

Or, les opérateurs de serveur racine sont représentés au sein du RSSAC. Mais il est important que le RSSAC ne soit pas impliqué dans des questions opérationnelles. Je pense que c'est une précision importante à faire. Il ne faut pas confondre, donc, ces entités.

Dans la structure de gouvernance de l'ICANN, le RSSAC fait partie des comités consultatifs, c'est le quatrième comité consultatif de l'ICANN et vous le voyez où est son rôle dans l'écosystème de l'internet.

En ce qui concerne l'organisation RSSAC, il est composé par des représentants nommés par les opérateurs de serveur racine. Il y

a aussi des agents de liaison avec d'autres opérateurs de zone racine et avec d'autres acteurs clés.

Nous avons également un caucus RSSAC. C'est un organe composé par des experts bénévoles. Les membres sont confirmés par le RSSAC en fonction de leur manifestation d'intérêt.

En ce moment, les coprésidents du RSSAC sont Brad Verd de Verisign, Tripti Sinha de l'Université du Maryland. Brad, il est là, il a levé sa main ; Tripti n'est pas là, peut-être qu'il est sorti un moment de la salle.

Au sein de RSSAC, nous avons plusieurs agents de liaison. On a une liaison de l'opérateur des fonctions IANA, du responsable de la maintenance de la zone racine. Vous avez vu le diagramme. Nous avons l'IANA, le responsable de la maintenance de la zone racine, le conseil d'architecture de l'internet. Nous avons également un agent de liaison de l'IAB. L'IAB est chargé de donner des orientations par rapport au modèle d'architecture de l'internet.

Au sein de l'ICANN, le RSSAC a des liaisons au sein du comité consultatif sur la stabilité et la sécurité, le Conseil d'Administration, le comité de nominations de l'ICANN, le comité permanent des clients, le comité de révision d'évolution

de la zone racine qui doit évaluer la performance des fonctions IANA qui sont assurées par la PTI.

Le comité de révision d'évolution de la zone racine est un comité qui a été créé dans le cadre de la transition de l'IANA pour évaluer l'évolution de la zone racine.

Pour ce qui est du caucus RSSAC, nous avons des experts techniques. Il y en a 88. Ils doivent présenter des manifestations d'intérêt qui sont publiques. Dans toutes les publications du RSSAC, les membres du caucus qui contribuent à ces travaux doivent être reconnus à la fin de la publication. Chaque contributeur est reconnu. Le caucus travaille de manière transparente par rapport à qui fait quoi. Le matériel ou la documentation est ouverte à tous ; vous pouvez accéder à ce matériel. Et nous avons des cadres, des processus de travail. Si vous êtes intéressés à participer au travail de ce caucus, il y a sur l'écran affichée l'adresse électronique à laquelle vous devez envoyer votre manifestation d'intérêt.

Le RSSAC a publié récemment des documents. Nous avons toute une série de publications numérotées. Nous sommes au RSSAC031. Nous avons récemment publié le RSSAC029 qui se penche sur les résultats de l'atelier du RSSAC tenu en octobre 2017. Le RSSAC030 est une déclaration sur les entrées dans les sources racine du DNS et le RSSAC031 est une réponse au

processus du groupe de travail PDP, c'est-à-dire processus d'élaboration de politiques sur les procédures pour des séries ultérieures de noms de domaine génériques de premier niveau. Le RSSAC tiendra une séance publique cette semaine. Je vous invite à y participer pour connaître davantage de détails par rapport à ces publications.

Quel est le travail en cours ? D'un côté, l'harmonisation des procédures de collecte de données concernant l'anonymisation. Le RSSAC a publié le RSSAC002. Les opérateurs ont mis en œuvre cela pour publier les statistiques sur le serveur racine et le système de serveur racine. Il y a un effort en court également pour essayer d'évaluer les procédures d'anonymisation. Et il y a également un autre travail en cours sur la taille des paquets et le DNS.

Depuis la restructuration du RSSAC en 2013, la transparence est un objectif important et nous essayons en permanence de l'améliorer. Nous avons fait quelques progrès en ce sens en établissant le caucus, en publiant les procès verbaux de nos réunions pour que la communauté de l'ICANN puisse comprendre où nous en sommes par rapport à notre travail et par rapport aux ateliers que nous tenons.

Il y a un calendrier pour le travail du caucus RSSAC où vous trouverez les différentes réunions que nous tenons ainsi que les

séances publiques. Nous avons des tutoriels et les agents de liaison se chargent de garantir que l'information puisse arriver aux bons destinataires.

Et finalement, le RSSAC a publié les procédures opérationnelles qui définissent le fonctionnement du RSSAC. Tout cela est publié sur le site web. Et nous en sommes à la troisième révision de ces principes opérationnels.

Les opérateurs de serveur racine essayent à leur tour d'améliorer leur transparence. Ils ont publié leur programme pour les réunions de l'IETF. Chaque opérateur racine doit publier les statistiques de leur travail et participent au RSSAC. Il y a aussi une page web et à partir de cette page web, vous pouvez accéder aux différentes pages web des différents opérateurs. Ils travaillent en coopération en cas d'évènements majeurs, par exemple l'attaque par déni de service qu'on a pu voir l'année dernière. Et cette page web sert à canaliser ces questions pour qu'elles arrivent aux bons destinataires.

Pour plus d'informations, vous voyez ici le lien vers la page web du RSSAC. Pour des questions générales, vous pouvez écrire à cette adresse électronique que vous voyez sur l'écran. Et vous voyez également le lien vers le caucus du RSSAC.

Et finalement, je voulais attirer votre attention sur le fait que le RSSAC a publié récemment sur son site web une partie

concernant les questions fréquemment posées, une foire aux questions. Et certaines de ces questions viennent justement des séances comme celle que nous tenons en ce moment.

Voilà un petit peu le travail du RSSAC. Maintenant, nous arrivons à la fin de notre présentation. Nous avons certains membres du RSSAC ici présents. J'aimerais les inviter à venir au podium pour qu'ils se présentent et pour qu'ils répondent à des questions que vous pourriez avoir. Très bien. Je vais inviter maintenant les membres du RSSAC ici présents à venir nous rejoindre au podium. Si vous avez des questions, levez la main, identifiez-vous, dites votre nom et posez votre question. Très bien. Je vais demander aux membres du RSSAC de se présenter.

FRED BAKER : Fred Baker, ISC.

JOHN CRAIN : John Crain, ICANN.

KAVEH RANJBAR : Kaveh Ranjbar, RIPE NCC.

BRAD VERD : Brad Verd, Verisign.

LARS-JOHAN LIMAN : Lars-Johan Liman, Netnod.

STEVE SHENG : Très bien. Nous allons commencer avec les questions.

CATHY PETERSEN : Nous avons une question en ligne de Jose de la Cruz. La question est la suivante : « Y a-t-il des plans pour étendre les entités pour qu'il y en ait plus de 13 ? »

STEVE SHENG : « Il y a des plans pour étendre des entités pour qu'il y en ait plus que 13 ? »

KAVEH RANJBAR : Tout d'abord, techniquement, ce serait possible d'élargir cela mais je pense que la question qu'il faut se poser, c'est pourquoi faudrait-il étendre cela. Du point de vue technique, si vous voyez la situation actuelle, ajouter des nodes ou ajouter des lettres ne fera pas une différence vraiment visible. La première question qu'il faut se poser, c'est que voulons nous faire en ajoutant de nouveaux identificateurs.

BRAD VERD : Je vais ajouter à cela que c'est une question que l'on nous pose régulièrement. Et la question de la part du RSSAC, c'est que nous essayons de voir si l'on doit ajouter ou même éliminer certaines de ces entités. C'est ce que nous évaluons et c'est un point qui se trouve dans notre liste de travail. Mais comme Kaveh l'a dit, faire cela viserait à résoudre un problème technique.

STEVE SHENG : Merci Kaveh et Brad. Je vais maintenant ouvrir le micro à des questions des personnes ici présentes. Le monsieur.

CATHY PETERSEN : Merci de bien vouloir dire votre nom

ABDULKARIM OLOYEDE : Merci beaucoup. Je m'appelle Abdulkarim. Je viens du Nigéria. C'est la première fois que je viens à une réunion de l'ICANN, je suis boursier. Ma question concerne les serveurs racine parce que les serveurs racine, il y en a plusieurs avec la même adresse IP. Donc quel est le problème avec ces différents serveurs qui sont égaux ? Comment peut-on les différencier puisqu'ils ont la même adresse IP ?

FRED BAKER : C’est une question sur le fonctionnement de Anycast. Il y a eu une présentation par rapport à cela. Le point fondamental, c’est le routage. Le point fondamental, je répète, c’est le routage. Chacun de ces serveurs fournit son service, c'est-à-dire répond aux requêtes qui leur sont envoyées. Mais ces serveurs sont en relation avec les fournisseurs des services internet et annoncent leur adresse.

Alors quand il y a une requête qui va vers cette adresse, le routage est envoyé au serveur le plus proche. Et si ce serveur est en panne ou si on perd ce routage, cette adresse est retirée par le BGP et il y aura une autre instance qui va prendre le relai. Et donc le routage va se diriger vers un autre serveur. Et c’est la façon dont cela fonctionne.

Au pire des cas, imaginons – je ne sais pas si cela pourrait arriver – mais imaginons que l’adresse n’est plus disponible dans le routage parce qu’elle n’existe plus. Alors l’une des raisons pour laquelle nous avons 13 serveurs racine, c’est pour que quelqu'un qui veut résoudre une adresse dans leur ordinateur puisse aller interroger quelqu'un d’autre s’il y a un serveur qui est en panne.

STEVE SHENG : Liman ?

LARS-JOHAN LIMAN : J'aimerais ajouter que quand nous utilisons Anycast, tous les serveurs ont deux adresses IP. Une des ces adresses IP est la même pour tous les ordinateurs. Et c'est ce qui est utilisé pour le trafic DNS. En outre, chaque serveur possède une adresse unique et séparée. Et cela est utilisé par les opérateurs pour pouvoir y arriver, à leur tour, à ces serveurs.

JOHN CRAIN : Je pense qu'il y a également une requête DNS différente où chaque instance a un nom que vous pouvez interroger dans le DNS. Je pourrai vous montrer cela si cela vous intéresse.

STEVE SHENG : Merci pour cette question et pour les réponses. Le monsieur qui est au fond de la salle ?

ORATEUR NON-IDENTIFIÉ : Je viens d'Inde. Une partie de la sécurité du DNS est assurée par le DNSSEC. Pouvez-vous nous dire dans quels pays le DNSSEC a été complètement déployé ? Et pouvez-vous nous dire s'il y a eu des problèmes associés à cette mise en œuvre ?

STEVE SHENG : Question sur le déploiement DNSSEC. Il y a un atelier du DNSSEC mercredi. Je pense qu'au début, ils vont vous montrer la

quantité de pays qui ont déployé le DNSSEC autour du monde. Donc ce serait une séance où vous pourrez trouver toutes ces informations.

BRAD VERD : Ce n'est pas véritablement dans notre portée mais peut-être que vous pourriez paraphraser cette question et la lier un peu plus à la racine. Peut-être qu'on pourrait y répondre.

KAVEH RANJBAR : Alors pour préciser, ce que nous publions en tant qu'opérateur de zone racine est le fichier de zone racine, c'est-à-dire le fichier qui est signé, c'est-à-dire que les opérateurs de zone racine, en général, commencent à travailler avec des données qui sont déjà signées. Et nous faisons la distribution de ce fichier. Ce n'est pas nous qui signons quoi que ce soit. Tout ce que nous faisons est de distribuer ce fichier qui est déjà signé, que nous sachions que l'intégrité de ce fichier est toujours assurée. Et c'est ce que nous vérifions au moment de distribuer les contenus de ce fichier.

STEVE SHENG : Merci. Y a-t-il d'autres questions dans la salle ? Oui, monsieur.

TARAU BAUIA : Je suis de Kiribati. J'ai une question. Lorsque nous déployons le DNSSEC, se pourrait-il qu'il y ait des problèmes avec des noms de domaine enregistrés sous le .com qui n'aient pas assuré l'intégrité de leur nom vis-à-vis du DNSSEC ? Est-ce un problème ?

STEVE SHENG : Oui, cette question correspond plutôt au DNSSEC et je pense qu'elle serait plus appropriée pour l'atelier du DNSSEC de mercredi. Donc je vous invite à participer à cet atelier. Venez me voir à la fin de la séance et je vous dirai exactement les détails de cet atelier.

Attendez, j'ai une question en ligne et puis vous êtes le suivant.

CATHY PETERSEN : J'ai une autre question de Jose de la Cruz qui demande : « Qui peut participer au RSSAC ? »

STEVE SHENG : Vous voulez répondre ?

BRAD VERD : Le RSSAC a un caucus de plus de 80 membres en ce moment. Ce sont des experts en la matière. Et en général, tous les membres ou toutes les équipes de travail sont créées par le caucus ou

sous les hospices du caucus en tout cas. Et ici à l'écran, vous avez l'adresse de notre site web. Si vous voulez consulter les membres du caucus ou si vous voulez rejoindre le caucus, vous pourriez contacter l'adresse email. Il y aura un groupe qui va vérifier votre candidature. Il faudra signer une manifestation d'intérêt et vous pourrez devenir une partie du caucus et donc une partie de la solution.

STEVE SHENG : Merci Brad et merci Jose de nous poser cette question.

KAVEH RANJBAR : Steve, si vous me permettez, je voudrais réitérer quelque chose. La plupart du travail technique du RSSAC est accompli au sein du caucus, c'est-à-dire que si vous êtes un membre du caucus, vous faites partie de la solution, vous faites partie du travail. Donc comme on nous a montré tout à l'heure dans les diapositives, il y avait 13 opérateurs qui font la plupart de travail de gestion ou d'administration.

Lorsqu'on reçoit un question ou qu'il est nécessaire de formuler un avis, le travail se fait au sein du caucus et tous nos membres du comité du RSSAC font également partie du caucus du RSSAC, c'est-à-dire que si vous voulez participer à la résolution du problème, vous pourrez joindre également un groupe de travail,

une équipe de travail. Mais chaque équipe de travail est formée par le caucus et le travail, essentiellement, se fait au sein du caucus.

BRAD VERD : Et le travail est également formulé au fait par les personnes qui font partie du caucus. Il n'est pas que le caucus fait le travail et d'autres, en fait, vont être reconnus ou remerciés.

STEVE SHENG : Merci. Oui.

ABDULKARIM OLOYEDE : Encore une fois, j'ai une autre question. Je voudrais savoir quelle est la fréquence des réunions du RSSAC et la fréquence des réunions du caucus ?

BRAD VERD : Le RSSAC se réunit une fois par mois. Nous tenons des appels mensuels. Il y a des procès verbaux de chaque réunion et les différentes questions sont abordées au cours de ces appels. Nos procès verbaux sont publiés, n'est-ce pas ? Non ? Les procès sont publiés, oui, d'accord. Les réunions ne sont pas publiques. Les procès sont publiés. Et le RSSAC se réunit également ici dans le cadre des réunions publiques de l'ICANN. Et ces dernières

années, nous avons également organisé deux ateliers par an pour présenter notre travail sur l'extensibilité. Si cela vous intéresse, vous pouvez venir à notre réunion publique du RSSAC.

Pour ce qui est du caucus, le caucus travaille en ligne. Les équipes de travail travaillent constamment, c'est-à-dire que les travaux des différentes équipes pourraient organiser des appels hebdomadaires ou deux fois par semaine ou toutes les deux semaines ; cela va dépendre de la charge de travail. Mais les réunions du caucus en elles-mêmes se tiennes ici lors de l'assemblée générale ou la réunion générale annuelle. Et c'est le caucus qui décide de la fréquence de ses réunions. Donc nous avons conclu que le mieux était de se réunir lors des réunions générales annuelles et toutes les deux réunions de l'IETF. Donc en fait, ce sont les réunions paires de l'IEFTF. C'est à ces réunions-là que le caucus va se réunir.

STEVE SHENG : Merci. Et donc la prochaine réunion du caucus sera lors de la réunion 102 de l'IETF à Montréal. Merci.

D'autres questions ? Oui, monsieur à gauche.

BONNIE MTENGWA : Bonjour, je m'appelle Bonne Mtengwa. Je viens de l'organisme de règlementation des télécommunications du Zimbabwe. Et

l'un de nos serveurs racine est situé au Zimbabwe. Je voulais savoir si les serveurs de noms vont être hébergés suivant les négociations des pays ou si c'est l'ICANN qui accorde ce privilège. Comme cela fonctionne ?

STEVE SHENG : Merci. Donc en fait, la question est par rapport à l'hébergement de l'instance de la zone racine. Liman ?

LARS-JOHAN LIMAN : La plupart des opérateurs de serveur racine ont des nuages Anycast et sont prêts à tenir des négociations par rapport à où les héberger. Ce n'est pas une question de négociations entre le pays et l'opérateur de serveur racine ; c'est des discussions avec les opérateurs spécifiques. Donc très souvent, ce sont des points d'échange de trafic internet et de grands fournisseurs de service internet.

Mais vous avez tout à fait raison, il y a des exigences à respecter, tout à fait. Pour la plupart des cas, il s'agit d'exigences techniques et financières. Nous travaillons sur la consolidation d'une liste de points de contact mais je vous conseille de contacter les opérateurs de serveur racine pour que l'on essaye de vous expliquer comment nous voyons la relation et quelles sont les exigences de notre côté. Je suis sûr que les autres

pourront faire la même chose à leur tour mais cela dépend un peu de l'environnement. Donc il faudrait voir si on arrive à trouver un moyen de respecter les exigences parce qu'il y a des exigences, tout à fait, oui.

STEVE SHENG : Merci Liman.

Y a-t-il d'autres questions ? Oui, monsieur ici.

ABDULKARIM OLOYEDE : Pardon, je suis encore Abdulkarim. Je me disais que le serveur racine et le DNS sont des parties importantes de l'internet, certes, et que le fonctionnement de tout ce système semble être très ouvert. Et on parle de personnes qui voudraient pouvoir attaquer les serveurs de noms. Et si tout le monde peut participer aux réunions, tout le monde peut contribuer, comment faites-vous pour éviter que les personnes qui veulent utiliser à mauvais escient le service le fassent ?

STEVE SHENG : Qui veut répondre ?

KAVEH RANJBAR : C'est une bonne question parce qu'on a différentes arêtes par rapport à cette question, différents aspects. Mais du point de

vue de RIPE NCC – et je pense qu'en général, tous les opérateurs de serveur racine seront d'accord – et c'est le fait qu'on ne peut pas garantir la sécurité de la racine si tout le monde ne participe pas. Donc on est très ouverts sur le fonctionnement et sur la conception même du DNS. Donc vous pourrez trouver des informations sur les instances. Très souvent, on publie ces informations. Même si elles ne sont pas publiées, il est très facile de comprendre le fonctionnement.

Donc le système est ouvert. Et nos capacités du point de vue technologique visent à garantir la réponse à tout type de requêtes. Et oui, c'est vrai qu'on reçoit beaucoup de requêtes illégitimes soi-disant pour nous attaquer peut-être. Mais en général, on a la capacité de pouvoir répondre aux bonnes requêtes.

JOHN CRAIN : Ces réseaux sont exploités par des professionnels, c'est-à-dire que tous les opérateurs ont des ingénieurs formés, des personnes qui sont des professionnels et l'intégrité de nos systèmes est quelque chose que nous tenons à cœur. C'est pourquoi lorsque vous hébergez une instance par exemple, il existe des exigences par rapport à qui peut accéder aux machines et comment ces personnes peuvent le faire, etc. Donc c'est quelque chose que nous prenons très au sérieux. Mais

comme le disait Kaveh, la conception du DNS est quelque chose de très ouvert. Donc je pense que c'est tout simplement la nature de notre protocole. C'est comme cela que ça fonctionne.

STEVE SHENG : Merci.

BRAD VERD : Pour ajouter ici à votre question, je pense que vu que le RSSAC et le caucus du RSSAC sont ouverts et que tout le monde peut nous rejoindre, rien n'empêche les délinquants de nous rejoindre. C'est ce que vous voulez dire ?

Et je pense que oui, c'est un risque, c'est vrai parce que nous voulons travailler de manière ouverte et transparente et nous voudrions connaître les différents points de vue des personnes pour pouvoir parvenir aux bonnes solutions pour tous les problèmes techniques que nous affrontons. Et en tant que coprésident du groupe, je dirais qu'on espère avoir suffisamment de frein et contrepoids, suffisamment de systèmes pour vérifier la bonne foi des personnes qui veulent participer pour pouvoir savoir ce qui se passe. Mais que je sache, ce n'était jamais le cas, on n'a jamais eu de personnes ou de délinquants qui nous rejoignent mais oui, c'est un risque, absolument.

ORATEUR NON-IDENTIFIÉ : Je suis [inintelligible], je viens de l'Inde. Je voudrais rebondir sur ce que vous disiez tout à l'heure lors de la présentation. Vous parliez du fait que le routage du trafic est déterminé non pas par la zone ou par le serveur mais que c'est les routeurs en fait qui vont le déterminer. Dans les exigences RSSAC002, vous parliez du fait que les opérateurs de serveur racine sont tenus de publier des statistiques du serveur racine. Donc je voudrais savoir, pour décider ou déterminer le trafic total dans un emplacement ou un pays déterminé, comment pourrais-je extrapoler ces données ? Ou alors comment pourrais-je trouver ces résultats à partir des statistiques qui sont disponibles en ligne des différentes sources à code ouvert ?

BRAD VERD : Merci. Je pense que la réponse la plus simple serait de vous dire que ce n'est pas possible. Le trafic du DNS de la racine ne devrait pas être utilisé comme une mesure du trafic internet total.

ORATEUR NON-IDENTIFIÉ : Non. En fait, ma question est : comment pourrais-je estimer ou avoir un résultat approximatif de ce trafic par remplacement ? Comment utiliser ce trafic du DNS pour parvenir à ces résultats ?

KAVEH RANJBAR : En général, pour avoir des résultats approximatifs utiles, on ne veut pas utiliser le DNS. Ce n'est pas le but du DNS. Mais il y a d'autres techniques possibles. Par exemple Google M-Lab mesure le trafic et ils essaient d'estimer le reste du trafic pour un pays ou pour une région. Il y a d'autres projets ; c'est ce que je veux dire. Mais le DNS n'est pas la bonne plateforme pour le voir. Les contenus ne passent pas par le DNS. Mais les informations par rapport au DNS à tout niveau, surtout au niveau de la racine, il y a beaucoup de résolveurs qui ont des informations en cache. Et cela n'est pas visible pour nous. Donc en fait, c'est impossible de savoir, même à un niveau approximatif, quel est le trafic.

FRED BAKER : Pour compléter en fait, lorsque vous accédez à un système de serveur racine et qu'on vous dit : « J'ai reçu cette quantité de requêtes IPv6. », entre autres, on vous demande en fait par rapport aux requêtes à la racine. C'est-à-dire qu'il y a des personnes qui essaient de trouver les adresses sous le .com, sous le .net mais on ne parle pas des emplacements particuliers ou de compagnies individuelles On parle de registres, tout simplement, c'est-à-dire que les données ne sont pas les bonnes.

STEVE SHENG : Merci. Y a-t-il d'autres questions ? Ya-t-il des questions en ligne ?

CATHY PETERSEN : Non, plus de question à distance.

STEVE SHENG : Nous avons une autre question dans la salle.

ABDULKARIM OLOYEDE : Abdulkarim encore une fois, pardon. Mais pour ce qui est du RSSAC et de l'organisation du renforcement de capacités, est-ce que vous organisez ce type d'ateliers de renforcement de capacités pour les personnes qui viennent de pays en développement ou pour celles qui sont intéressées ? Parce que souvent, par exemple une personne qui est intéressée mais qui n'a jamais vu un serveur racine de sa vie, qui voudrait savoir ce que vous faites, cette personne se retrouve avec des informations trop techniques. Et donc on n'a pas moyen de savoir plus, de pouvoir satisfaire à cette inquiétude.

KAVEH RANJBAR : Je ne suis pas sûr d'avoir bien compris la question. En tant que boursier et assistant pour la première fois, merci d'être aussi impliqué. C'est très encourageant.

Par rapport au renforcement des capacités, chaque opérateur de serveur racine pourrait avoir ses propres plans. Par exemple

au nom de RIPE NCC, nous sommes un registre international RIR d'Europe, Moyen Orient et l'Asie centrale. Donc non seulement dans notre région mais dans le reste du monde c'est-à-dire en Afrique, dans la région Asie-Pacifique, nous travaillons avec d'autres RIR. Dans le cas par exemple de l'Afrique, nous avons un protocole d'accord avec AfriNIC et avec APNIC dans le cas de l'Asie-Pacifique.

Mais suivant cet exemple de l'Afrique, avec AfriNIC, en Afrique, AfriNIC a créé et a établi une alliance avec ISOC Afrique. Et ils sont en train de chercher des bailleurs de fonds pour avoir du financement nécessaire. Il parle avec différentes parties impliquées pour pouvoir organiser ce type d'atelier de renforcement des capacités dans le cadre d'ISOC Afrique, entre autres.

Donc vous voyez que nous avons différentes méthodes. Chacun a ses propres méthodes pour former les participants dans sa région. Donc il faudrait que vous en discutiez avec les différents opérateurs de la zone racine. Mais on le demandait tout à l'heure, comment faire pour avoir une instance de serveur racine ? Il existe un site web où vous avez une liste de chaque opérateur et vous trouverez, à côté du nom de l'opérateur, l'adresse web pour chaque service, donc les services Verisign pour la racine ou autres. Mais tous les RIR sont énumérés sur

cette page web et vous pourrez des informations pour les contacter.

BRAD VERD : Un bon nombre de ces questions sont plutôt opérationnelles et il y a ici des opérateurs de zone racine, également. Mais en tout cas, RSSAC fournit des conseils, des avis sur le système au Conseil d'Administration. Et un bon nombre de ces questions ne portent pas sur RSSAC. Nous sommes prêts à y répondre, nous devons être aussi transparents que possible mais il faudrait maintenir la distinction entre le RSSAC et les opérateurs de la racine. D'accord ? Merci.

STEVE SHENG : Merci.

Y a-t-il d'autres questions ? Non ? Ah, Liman.

LARS-JOHAN LIMAN : Si vous avez des questions qui vous viennent à l'esprit à la fin de la séance, venez-nous parler. Au moins, je parle en mon propre nom Je ne sais pas quel est le cas avec le reste de la tribune ici mais au moins moi, je serai prêt à vous donner les réponses que je pourrai vous donner, où que ce soit.

BRAD VERD : Oui et moi aussi, je voulais attirer votre attention sur la foire aux questions qui a été publiée sur la page web récemment. Même si, comme je le disais tout à l'heure, un bon nombre de ces questions sont de type opérationnel, nous avons essayé de capturer toutes ces questions qui sont apparues à partir des différentes présentations de notre groupe. Et cette foire aux questions est en évolution constante, c'est-à-dire que s'il y a des questions qui n'y apparaissent pas, c'est sûr que votre question sera aussi un doute pour quelqu'un d'autre. Donc envoyez-la nous pour qu'on puisse l'ajouter.

STEVE SHENG : Voilà. Et je vous montre ici à l'écran le site web du RSSAC où vous voyez différentes sections. Donc on a réunions, caucus, publications et la FAQ, la foire aux questions. Lorsque vous accédez à ces liens, que vous les suivez, vous trouvez d'autres informations sur l'adhésion au RSSAC, sur les publications, l'adhésion au caucus, les réunions et la foire aux questions.

Le site web root-servers.org était le site dont je parlais tout à l'heure qui contient les points d'accès aux différents serveurs racine. Donc si vous avez des questions, des doutes, vous trouvez des informations de contact là-dessus et c'est également ici qu'apparaît cette carte que nous avons tirée pour notre présentation. Donc vous voyez que vous pourriez voir dans

plus de détails chaque région et voir davantage d'informations là-dessus.

Cela dit, s'il n'y a plus d'autres questions, je vais vous remercier d'avoir participé à cette séance. Je remercie les membres du RSSAC d'avoir répondu à vos questions. La séance est maintenant ajournée.

CATHY PETERSERN : Merci à tous.

[FIN DE LA TRANSCRIPTION]