SAN JUAN – Como funciona: Operação do servidor raiz
Segunda-feira, 12 de março de 2018 – 10h30 às 12h AST
ICANN61 | San Juan, Porto Rico

HOMEM NÃO IDENTIFICADO: Bom dia. ICANN 61, Como funciona: Operação do servidor raiz, 12 de março

CATHY PETERSEN: Bom dia a todos. Bem-vindo a Como funciona. Estamos um pouco atrasados depois daquela maravilhosa cerimônia de abertura, então sejam pacientes. Começaremos em breve. Obrigado.

HOMEM NÃO IDENTIFICADO: Ei, pessoal. Começaremos em aproximadamente dois ou três minutos. Começaremos com 15 minutos de atraso porque a cerimônia de abertura se alongou um pouco. Mas se puderem se preparar para começarmos em dois ou três minutos, seria ótimo.

CATHY PETERSEN: Bom dia a todos, novamente. Bem-vindo a Como funciona. Nesta sessão, falaremos sobre Operações de servidor raiz.

Agradeço novamente pela paciência. Andrew McConachie é nosso primeiro palestrante. Andrew?

ANDREW MCCONACHIE: Obrigado. Olá, meu nome é Andrew McConachie. Eu trabalho no Apoio a políticas da ICANN, dando suporte ao RSSAC. Falarei sobre o sistema de servidor raiz.

Primeiro, algumas linhas gerais. Teremos quatro sessões hoje: visão geral do sistema de nomes de domínio, o sistema de servidor raiz atualmente e seus recursos. Depois, passarei a palavra ao meu colega Steve Sheng, que dará uma explicação sobre o Anycast e depois falará sobre o RSSAC e algumas de suas atividades recentes.

Em seguida, teremos um período de perguntas e respostas no qual alguns dos operadores de servidor raiz que estão na sala virão até o palco para responder a suas dúvidas. Portanto, reservem suas perguntas para o final.

Vamos começar com uma visão geral do sistema de nomes de domínio e dos servidores raiz. Uma breve recapitulação: o que são endereços IP e como eles funcionam como identificadores na Internet? Os endereços IP são o identificador fundamental na Internet e todos os hosts conectados à Internet precisam ter endereços IP. Quer seja IPv4 ou IPv6 ou se você estiver operando

por meio de um NAT, ainda assim será necessário um endereço IP. Endereços IP são um rótulo numérico. Eles não são realmente de fácil compreensão, são apenas números.

Por que precisamos de DNS? Bem, o problema original é que, como mencionei no slide anterior, os endereços IP são difíceis de lembrar e mudam muito. Assim, o problema original com DNS era apenas ter alguns nomes fáceis de lembrar que pudéssemos associar a endereços IP para que não fosse necessário lembrar dos endereços IP.

Esses problemas permanecem, mas existem também alguns problemas mais modernos, como o fato de endereços IP poderem ser compartilhados e vários endereços IP poderem ser associados a um único serviço. Portanto, temos esse problema moderno, tanto de muitos para um quanto de um para muitos, adicionado ao problema original de apenas os endereços IP serem realmente difíceis de lembrar.

Agora o sistema de nomes de domínio é hierárquico. Como vocês podem ver no diagrama, no topo temos uma raiz. Abaixo disso, temos o que chamamos de domínios de primeiro nível ou TLDs. Alguns exemplos incluem .edu, .mil, .uk. Então, abaixo disso, temos o que algumas pessoas chamam de segundo nível e depois o terceiro nível e assim por diante. Esses são chamados de mapeamentos de endereços IP. É com isso que estamos mais

familiarizados, mas há outros mapeamentos, como registros MX para servidores de e-mail, registros reversos, às vezes chamados de registros PTR, que mapeiam de endereços IP de volta para nomes.

Este slide é bem complicado. Passarei algum tempo explicando-o. Este slide tem o objetivo de mostrar o processo de resolução de DNS, como um usuário experiencia o DNS, pelo que um usuário passa, as várias etapas, o fluxo do que significa interagir com o DNS para que um usuário possa resolver um nome de domínio para um endereço IP e, finalmente, chegar a um site.

Temos um usuário aqui, à direita. Ele realmente quer acessar www.exemplo.com como um servidor Web. A primeira coisa que ele faz é abrir o navegador da Web. Isso aciona uma solicitação de DNS que vai para o que chamamos de servidor de nomes recursivo. Supondo que o servidor de nomes recursivo não tenha nada em seu cache e, nesta demonstração, vamos supor que alguém acabou de ativar esse servidor de nome recursivo, o cache está vazio, não sabe de nada. O que ele faz?

Ele acabou de receber uma consulta para www.exemplo.com e tem um monte de trabalho a ser feito antes de retornar uma resposta ao usuário. A primeira coisa ele que faz é ir até a raiz e dizer: “Este é www.exemplo.com. Onde ele está?” A raiz diz: "Eu não sei onde está isso, mas sei onde está .com". Assim, ela

retorna ao servidor de nomes recursivo o endereço dos servidores de nomes .com.

Em seguida, o servidor de nomes recursivo vai até os servidores de nomes .com e diz: "Onde está www.exemplo.com?" Os servidores de nomes .com dizem: "Não sei onde está isso, mas sei onde está o servidor de nomes exemplo.com. Está aqui."

Em seguida, o servidor de nomes recursivo acessa os servidores de nomes exemplo.com e diz: "Onde está www.exemplo.com?" Por fim, ele recebe a resposta que está procurando e o servidor de nomes recursivo é capaz de responder ao usuário com o endereço www.exemplo.com.

É assim que um usuário passará por todo o processo de resolução desse nome de domínio para um endereço IP e, finalmente, poderá acessar a página da Web.

Há outra coisa sobre o qual não falei neste slide, que é o aspecto de segurança, as DNSSEC, também chamadas de aspecto de segurança do DNS, que está em cada uma dessas perguntas entre o servidor de nomes recursivo e cada um desses servidores de nomes oficiais — o servidor de nomes raiz, o servidor de nomes .com e o servidor de nome exemplo.com — essas respostas que retornam ao servidor de nome recursivo desses servidores oficiais são assinadas e o servidor de nome recursivo é capaz de validar se elas são as respostas corretas. Se a

resposta não foi adulterada. Que ela não foi dada pelo servidor de nomes oficial incorreto. Essa é a resposta correta e é possível fazer isso por meio das DNSSEC.

Esse é o processo de resolução do sistema de nomes de domínio. Como vimos no slide anterior, os servidores raiz só sabem quem precisa ser perguntado a seguir. Eles só têm os endereços dos servidores de nome do TLD, como .com, .net e .org. No entanto, eles geralmente não perguntam isso com frequência.

No exemplo anterior que apresentei, tivemos essa situação hipotética na qual o servidor de nomes recursivo havia acabado de ser ligado e não tinha nada em seu cache. Bem, isso é bem raro. Os servidores de nomes recursivos têm um cache bastante extenso, e a grande maioria das consultas enviadas aos servidores de nomes recursivos são respondidas fora do cache. Isso significa que há muito menos consultas na raiz do que você imagina originalmente.

Alguns refinamentos modernos no DNS. Eu já falei sobre as DNSSEC, também chamadas de segurança de DNS ou extensões de segurança. O objetivo das DNSSEC é assinar respostas que são enviadas aos servidores de nomes recursivos para que o servidor de nomes recursivo possa validá-las. Por validação, quero dizer que ele pode assegurar que a resposta está correta

porque foi assinada por uma chave por meio de criptografia, então ele pode garantir que a resposta está correta.

Também houve aprimoramentos de privacidade, e eles ainda estão sendo muito trabalhados na Força-tarefa de Engenharia da Internet. Algo como DNS sobre segurança da camada de transporte, que vai assegurar a transmissão da consulta pela rede e garantirá que os olhos curiosos não a vejam. Esses ainda estão em desenvolvimento ativo.

Outro refinamento moderno do DNS é o Anycast. Anycast é muito usado pelos operadores do servidor raiz. O Anycast basicamente faz duas coisas importantes: permite que vários servidores compartilhem um único endereço IP e protege contra ataques de DDoS. Meu colega Steve Sheng falará mais tarde sobre o Anycast e como isso acontece.

A zona raiz em relação aos servidores raiz. A zona raiz é composta dos dados que os servidores raiz atendem. Você pode pensar na zona raiz como o ponto de partida. Ela é a lista de TLDs e servidores de nomes, é o topo da hierarquia ou da árvore. Ela é gerenciada pela ICANN de acordo com a política da comunidade. Ele é compilado e distribuído pelo mantenedor da zona raiz para todos os operadores do servidor raiz. Novamente, é o conteúdo do banco de dados dos operadores do servidor raiz. São os dados que aos quais servidores raiz atendem.

Por outro lado, os servidores raiz respondem com dados da zona raiz. Atualmente, há 13 identidades e mais de 900 instâncias em diversos locais físicos em todo o mundo. Os servidores raiz são puramente um papel técnico. Eles atendem aos dados da zona raiz. Cada uma dessas nuvens do Anycast executadas pelos operadores do servidor raiz são de sua própria responsabilidade.

Analisando um pouco mais sobre o que é um operador de servidor raiz, existem 12 grupos de profissionais de engenharia diferentes que estão focados na confiabilidade e estabilidade do serviço e na acessibilidade para todos os usuários da Internet. Eles são profissionais e cooperam entre si, agindo de maneira independente, são um grupo diversificado de organizações. Com isso, quero dizer que eles são tecnicamente, organizacionalmente e geograficamente diversos.

No entanto, os operadores não estão envolvidos na elaboração de políticas nem em modificações de dados. Eles apenas atendem aos dados da zona raiz. Eles estão envolvidos na operação cuidadosa do serviço, em atender a esses dados, avaliar e implantar novas modificações técnicas — portanto, novos padrões podem surgir da Força-tarefa de Engenharia da Internet — além de assegurar que o serviço permaneça estável, robusto e acessível para todos os usuários na Internet.

Isso foi um pouco sobre o DNS, um tanto técnico, mas provavelmente não muito técnico. Agora vamos falar sobre o sistema de servidores raiz hoje e a respeito de alguns de seus recursos.

O crescimento do sistema do servidor raiz. Este slide mostra um pouco da história dos números dos servidores raiz, as identidades dos servidores raiz ao longo dos anos desde a década de 1980. Vocês podem ver que houve progresso.

De 1998 até agora, temos 13 identidades diferentes. Essas mudanças têm respondido principalmente a demandas técnicas, bem como a problemas de dimensionamento. Atualmente, os problemas de dimensionamento são realmente resolvidos pelo Anycast. O Anycast é simplesmente uma ferramenta maravilhosa na caixa de ferramentas dos operadores de servidores raiz para lidar com problemas de dimensionamento.

Atualmente, os servidores raiz estão todos operando IPv6 e IPv4, portanto, há 13 pares de endereços IPv4 e IPv6. Mais uma vez, existem mais de 900 instâncias individuais.

Esses são alguns dos princípios fundamentais do sistema de servidores raiz. Há cinco deles. É importante que esse sistema de servidores raiz forneça uma plataforma estável, confiável e resiliente para o DNS; que ele opere para o bem comum de toda

a Internet; que a IANA seja a origem dos dados raiz do DNS — ou seja, os dados da zona raiz; e que as alterações na arquitetura sejam feitas com base nos resultados da avaliação técnica e da necessidade técnica demonstrada; e que a operação técnica e as expectativas do DNS sejam definidas pela Força-tarefa de Engenharia da Internet.

Se estiver interessado em um pouco mais do histórico do sistema de servidores raiz, você pode fazer o download e ler o RSSAC023, History of the Root Server System, no site do RSSAC.

Esses são os operadores do servidor raiz atualmente. Observamos que há 13 identidades. Os nomes de host deles estão listados à esquerda. Vocês observam na coluna do meio os endereços IP. Há IPv4 e IPv6 para todos eles. Cada um desses endereços IPv4 e IPv6, bem, pelo menos todos os endereços IPv4, resultam em uma nuvem do Anycast. Então, por trás desses endereços IP, há muitos, muitos servidores — mais de 900 neste momento, mas estão em constante crescimento. No último ICANN, quando fiz esta apresentação, eu dizia que existem mais de 800 instâncias e agora estou dizendo que há mais de 900 instâncias. Então, elas estão crescendo constantemente.

Aqui está uma visão dos servidores raiz atualmente. Isso foi retirado do site root-servers.org. É apenas uma visão geral de

onde estão os servidores raiz. Não é necessariamente preciso. Não há a informação de que há exatamente, por exemplo, sete instâncias de servidores raiz em Madagascar. É um gráfico. É um tanto interessante. Você pode obter informações mais detalhadas no site. Você pode até mesmo consultar as cidades nas quais cada instância está em cada um dos operadores. Esta é uma visão geral muito ampla, mas se acessar o site, você poderá realmente obter mais detalhes e algumas informações interessantes.

Essa é a estrutura de gerenciamento da zona raiz. É assim que os dados da zona raiz, a zona raiz, chegam aos servidores raiz. Digamos que você seja um operador de TLD e precise fazer uma alteração na zona de raiz. Talvez seus registros de NS mudem. Talvez as associações mudem. Você precisa alterar algumas das informações associadas a alguns dos registros de seu TLD.

Então você acessa a IANA e faz essa alteração, e essa mudança será passada para o mantenedor da zona raiz, que atualmente é a Verisign. Então, acredito que, duas vezes por dia, eles distribuirão essa alteração, distribuirão toda a zona de raiz para os operadores do servidor raiz. Depois, os operadores do servidor raiz serão responsáveis por levar isso para toda a nuvem do Anycast e, em seguida, atenderão ou responderão às consultas que chegam de todos os resolvedores recursivos.

Alguns dos recursos dos operadores de servidores raiz: há uma diversidade de estruturas organizacionais, seu histórico operacional é algumas vezes diferente, eles usam hardware e software diferentes. Eles usarão plataformas de hardware diferentes, bem como plataformas de software diferentes, o que ajuda em termos de segurança, pois há uma forte correlação entre melhor segurança e maior diversidade. Eles também têm diferentes tipos de modelos de financiamento e são tipos diferentes de organizações que recebem financiamento de diferentes maneiras.

No entanto, eles compartilham algumas práticas recomendadas: segurança física robusta, superprovisionamento de sua capacidade de lidar com ataques de DDoS, além de lidarem com picos de tráfego e todos terem uma equipe profissional e confiável.

Eles cooperam por meio de várias reuniões do setor na comunidade. A ICANN é uma delas, mas também a Força-tarefa de Engenharia da Internet, NOGs como NANOG ou RIPE, DNS-OARC, que é um grupo operacional e de pesquisa. Eles também usam ferramentas de colaboração baseadas na Internet e são transparentes em suas operações.

Além disso, eles coordenam a preparação para emergências a fim de proteger a infraestrutura em caso de emergências

catastróficas ou outros tipos de emergências. Eles têm atividades periódicas para apoiar a resposta a emergências. Não posso ler o último item porque ele está cortado.

Respostas a uma Internet em evolução. À medida que a Internet evolui, novos requisitos são colocados no sistema DNS. Com o tempo, os operadores de servidores raiz adotaram o IPv6, o Anycast e as DNSSEC. Os Nomes de Domínio Internacionalizados também são mencionados aqui porque há muitos IDNs na zona raiz. O importante é aumentar a eficiência, a capacidade de resposta e a resiliência. Mais uma vez, existem mais de 900 instâncias de Anycast implantadas atualmente.

Alguns dos mitos que as pessoas podem ter, alguns dos equívocos que as elas podem ter sobre o sistema de servidores raiz. Primeiro mito, os servidores raiz controlam a direção do tráfego da Internet. Isso não é totalmente verdadeiro. Na verdade, isso é um mito. Os roteadores realmente controlam a direção do tráfego da Internet. Acho que talvez esse mito possa ter acontecido porque o DNS associa nomes a endereços IP, mas, em última análise, são os roteadores baseados em endereços IP que controlam para onde vão os pacotes.

Outro mito é que a maioria das consultas de DNS são tratadas por um servidor raiz. Como observamos no exemplo, isso pode ser verdade se o cache de servidores DNS recursivos estiver

vazio, mas isso raramente ocorre. Portanto, a maioria dos servidores DNS não é controlada por um servidor raiz. A maioria deles é controlada fora do cache do recursivo.

A ideia de que a administração da zona raiz e o provisionamento de serviços são a mesma coisa é outro mito. Isso não é verdadeiro. No diagrama que mostrei anteriormente sobre a divisão de responsabilidades e como uma mudança chega até os servidores raiz, há diferentes partes envolvidas lá.

Outro mito é que as identidades do servidor raiz têm um significado especial. Na verdade, eles não têm. Ou que existem apenas 13 servidores raiz. Existem mais de 900.

Outro mito seria que os operadores de servidores raiz conduzem operações de maneira independente. Embora sejam organizações independentes, há muita coordenação e cooperação para assegurar o serviço estável do sistema de servidores raiz como um todo.

O mito final é que os operadores do servidor raiz recebem apenas a parte do TLD de uma consulta. Isso também não é verdade. Eles recebem toda a consulta. É assim que o DNS funciona. Há um trabalho na Força-tarefa de Engenharia da Internet para mudar isso. Se você estiver interessado, a palavra-chave é a minimização de QNAME e você pode ler sobre esse

trabalho, onde os servidores raiz podem receber apenas a parte superior da consulta.

Agora, vou passar a palavra ao meu colega Steve Sheng, que apresentará as duas últimas seções, começando pelo Anycast.

STEVE SHENG: Obrigado, Andrew. Meu nome é Steve Sheng. Também sou da equipe de políticas que dá apoio ao RSSAC. Darei uma explicação sobre o Anycast e também sobre o RSSAC e suas atividades.

Anycast é um termo de roteamento e endereçamento. Há dois termos aqui: Unicast e Anycast. Existem diferenças importantes. No Unicast, todos os pacotes ou datagramas de origens são enviados ao mesmo destino e uma única instância atende a todas as origens. Portanto, no caso de um ataque de negação de serviço, todo o tráfego de ataque é enviado para essa única instância. Isso é Unicast.

Por outro lado, no Anycast, as várias instâncias servem aos mesmos dados para todas as origens. Essas várias instâncias têm o mesmo endereço IP e as políticas de roteamento intermediárias determinam o destino com base na origem. Isso significa que a origem obtém os dados mais rapidamente, chega

ao destino mais próximo e o tráfego de ataque de DDoS é enviado para a instância mais próxima.

Deixe-me ilustrar isso com um diagrama.

Aqui, na ilustração do Unicast, vocês observam uma origem e um destino identificados. O destino é uma instância única e o tráfego usa a rota mais curta até o destino único.

Aqui, no Anycast, vocês observam os três destinos em azul. Todos esses destinos anunciam o mesmo endereço IP e as políticas de roteamento determinam o mais próximo, da origem até o destino. Isso significa que o caminho da origem ao destino é reduzido e os dados são entregues mais rapidamente.

Como isso ajuda contra os ataques de negação de serviço? Em um ataque de negação de serviço, um invasor ataca o destino. Mas como há Anycast, o tráfego só chega até o link mais próximo. Portanto, talvez um dos links de destino esteja sobrecarregado, mas o outro destino ainda serve ao tráfego.

Uma das perguntas que recebemos nessas sessões de tutoriais é sobre o sistema do servidor raiz e suas redes. Alguns de vocês são operadores de rede, outros podem operar instâncias recursivas. Se você é um operador de rede, deseja ter três ou quatro instâncias próximas. Isso aproxima as instâncias de você e, em alguns casos, reduz o tempo de ida e volta.

Acredito que, além disso, você também quer aumentar suas conexões e arranjos de peering. Às vezes, você observa que pode ter uma instância raiz perto de você, mas o tráfego ainda viaja pelo mundo para chegar até você. Isso ocorre devido às conexões e aos arranjos de peering. Então isso também é um fator importante.

Se você for um operador de resolvedor recursivo, para aumentar o armazenamento em cache, considere implementar a tecnologia RFC7706. Ela executa uma cópia da zona raiz em um endereço de retorno. O benefício disso é que algumas vezes ela reduz o risco de perda de privacidade do resolvedor recursivo até o servidor raiz.

Obviamente, é importante ativar a validação das DNSSEC nos resolvedores. Isso garante que você receba os dados não modificados da IANA em todo o processo, como Andrew mencionou, por meio dos dados corretos.

E, finalmente, acho que isso acontece porque estamos na ICANN, convidamos especialistas técnicos e outras pessoas para participar e contribuir para a Comissão do RSSAC. É onde o aconselhamento técnico do RSSAC é gerado e criado.

Com isso, deixe-me apresentar uma atualização rápida ou visão geral do RSSAC e de suas atividades recentes. RSSAC significa Comitê Consultivo do Sistema de Servidores Raiz. Ele é

encarregado de assessorar a ICANN, a comunidade e a diretoria em questões relacionadas à operação, à administração, à segurança e à integridade do sistema de servidores raiz da Internet. Observem que esse é um escopo muito restrito para este comitê consultivo.

Uma importante distinção que muitas vezes é confundida, especialmente na ICANN, é que o RSSAC é um comitê de aconselhamento, principalmente para a diretoria, mas também para outros órgãos e organizações da ICANN que se envolvem nos negócios gerais do DNS.

No entanto, os operadores do servidor raiz são representados no RSSAC. Porém, é muito importante observar que o RSSAC não se envolve em questões operacionais. Então, acho que essa é uma distinção muito importante para não confundir essas duas entidades.

Na estrutura geral de governança da ICANN está um dos quatro comitês consultivos, que está localizado no ecossistema da ICANN.

Dentro da organização, o RSSAC é composto pelos representantes designados ou pelos operadores de servidores raiz, e cada um pode indicar um substituto para o RSSAC. Ele também possui representantes para os parceiros de

gerenciamento da zona raiz e as principais organizações técnicas.

A Comissão do RSSAC que mencionei anteriormente é um corpo de especialistas voluntários. Seus membros são confirmados pelo RSSAC com base em uma declaração de interesse.

Os atuais presidentes do RSSAC são Brad, da Verisign, e Tripti, da Universidade de Maryland. Brad e Tripti, vocês estão na sala? Vocês podem levantar as mãos. Esse é o Brad. Eu conheço Tripti, mas ela deve ter acabado de sair por um momento.

No RSSAC, há vários representantes. Um é o representante do operador de funções da IANA, o mantenedor da zona raiz. Andrew mostrou esse diagrama, o fluxo de gerenciamento da zona raiz, a IANA e o mantenedor da zona raiz. Eles são as duas entidades essenciais.

O RSSAC também tem contatos do Conselho de Arquitetura da Internet. Isso fornece orientação de arquitetura para a Sociedade da Internet e a IETF em assuntos relacionados à arquitetura da Internet.

Na ICANN, o RSSAC tem representantes no Comitê Consultivo de Segurança e Estabilidade, na diretoria da ICANN, no Comitê de Nomeação, no Comitê Permanente do Consumidor, que é o

comitê encarregado de analisar o desempenho da função da IANA que atualmente é desempenhada pela PTI.

E, finalmente, o Comitê de Revisão de Evolução da Zona Raiz, um comitê criado como parte da transição da IANA para examinar os problemas de arquitetura para a evolução da zona raiz.

A Comissão do RSSAC tem atualmente 88 especialistas técnicos. Suas declarações de interesse são públicas. Em qualquer publicação do RSSAC para qualquer um dos membros da Comissão que contribuam ou liderem esse trabalho, eles são mencionados no final de cada relatório. Portanto, há crédito público para o trabalho individual.

Eles trazem diferentes conhecimentos para as publicações. E a Comissão é transparente em relação a quem faz o trabalho. A lista de discussão é aberta, então você pode ver os arquivos. Há também uma estrutura para que tudo seja realizado.

Se você estiver interessado em participar da Comissão do RSSAC, o e-mail correto para se inscrever é rssac-membership@icann.org.

Aqui estão algumas das publicações recentes do RSSAC. O RSSAC tem uma série de publicações. Essa é a numeração. Atualmente, eles estão no número 31. A última publicação

[gratuita] é o RSSAC029, que descreve o resultado do workshop de outubro de 2017. O RSSAC030 é uma declaração sobre entradas em fontes raiz do DNS.

E o RSSAC031 é uma resposta aos procedimentos subsequentes do PDP da GNSO. Trata-se do procedimento subsequente para criar novos TLDs. A resposta do RSSAC aborda um tópico sobre dimensionamento da raiz.

O RSSAC terá uma sessão pública esta semana. Por favor, participem para saber mais detalhes sobre essas publicações.

Sobre os trabalhos atuais, existem dois: Harmonização de procedimentos de anonimização para coleta de dados. O RSSAC publicou o RSSAC002 e os operadores de servidores raiz implementam isso para publicar estatísticas sobre os servidores raiz e o sistema do servidor raiz. Há [um esforço em andamento] para analisar o procedimento de anonimização de alguns desses dados. A outra equipe de trabalho refere-se aos tamanhos dos pacotes e o DNS.

Desde a reestruturação do RSSAC em 2013, a transparência é uma meta importante que está em processo de aprimoramento, e eles fizeram muito progresso com a criação da Comissão, publicando as minutas e os relatórios do workshop para que a

comunidade da ICANN possa entender o status atual do trabalho, os relatórios, as oficinas.

Há um calendário público do RSSAC e da Comissão com todas as várias reuniões da equipe de trabalho. Em cada reunião da ICANN, o RSSAC realiza sessões públicas. Temos os tutoriais e os relacionamentos de parcerias garantem que a informação flua para as principais organizações.

Finalmente, o RSSAC [codificou] os procedimentos operacionais que definem como o RSSAC opera. Isso também está no site. Acho que estamos na terceira revisão.

Os operadores do servidor raiz também tomam medidas para melhorar a transparência. As agendas das operações raiz são publicadas para as reuniões da IETF. Todo operador publica estatísticas do RSSAC002. Eles estão participando do RSSAC. Há uma página pública na Web, uma única página da Web, e, a partir dessa página, você pode acessar páginas da Web de operadores individuais. Eles colaboram em relatórios sobre eventos importantes. Por exemplo, os eventos de ataque de DDoS no ano passado. E o RSSAC atua como um gateway para canalizar essas questões para os operadores de raiz, que serão respondidas por eles.

Para obter mais informações, aqui está um link para a página da Web do RSSAC. Qualquer dúvida geral, vocês podem enviar para

esse endereço de e-mail. O link para a Comissão e associação está relacionado aqui.

Por fim, quero chamar sua atenção para o fato de que o RSSAC publicou recentemente em seu site as perguntas e respostas mais frequentes. Acredito que seja uma lista de 25 perguntas frequentes. Algumas delas são geradas a partir dessas sessões. Então, são muito úteis para entender o RSSAC.

Com isso, acho que chegamos ao final da apresentação. Temos alguns membros do RSSAC aqui. Eu gostaria de convidá-los a vir até o palco para se apresentar, e também vou moderar uma sessão de perguntas e respostas. Então, com isso, posso convidar os membros do RSSAC para subir ao palco.

Se vocês tiverem alguma dúvida, por favor, levantem a mão e eu vou identificá-los. Vamos fazer isso. Posso pedir primeiro aos membros do RSSAC que se apresentem, começando por Fred?

FRED BAKER: Fred Baker, ISC.

JOHN CRAIN: John Crain com ICANN.

KAVEH RANIBAR: Kaveh Ranibar, RIPE NCC.

BRAD VERD: Brad Verd com Verisign.

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

STEVE SHENG: Obrigado. Começaremos com uma pergunta on-line. Cathy?

CATHY PETERSEN: Temos uma pergunta on-line de Jose de la Cruz. A pergunta é: "Há planos de expandir as entidades para mais de 13?"

STEVE SHENG: "Há planos de expandir as entidades para mais de 13?" Quem gostaria de responder a essa pergunta?

KAVEH RANIBAR: Posso começar. Primeiro, tecnicamente deveria ser possível expandir. Essa é minha opinião pessoal. Mas acho que a verdadeira questão é por que devemos expandir o número de identificadores? Pois essas letras, basicamente, são identificadores. Porém, do ponto de vista tecnológico, se você observar a situação atual, adicionar nós ou letras não terá uma diferença técnica significativa ou visível. Então, a primeira

pergunta é sobre qual problema vocês estão tentando resolver com a adição de novos identificadores? Foi isso que entendi.

BRAD VERD: Vou acrescentar que essa é uma pergunta recorrente. Recebemos essa pergunta com bastante frequência e acredito que a resposta seja que o RSSAC está buscando não apenas adicionar, mas também remover alguns. Talvez 13 não seja o número correto. Pode ser mais ou menos do que isso. Não temos essa resposta. Esse é um dos itens que está na nossa lista de trabalho a ser abordada. Mas como disse Kaveh, nossa meta é buscar a solução para o problema técnico da pergunta. Obrigado.

STEVE SHENG: Obrigado, Kaveh e Brad. Com isso, abro as perguntas para o público. O senhor na frente.

CATHY PETERSEN: Por favor, vocês poderiam — apenas um lembrete — dizer seu nome e a afiliação, caso tenham alguma? Obrigada.

ABDULKARIM OLOYEDE: Muito obrigado. Meu nome é Abdulkarim, da Nigéria. Sou um novo fellow da ICANN. Minha pergunta é sobre os servidores

raiz, pois cada um dos 13 servidores raiz provavelmente está duplicado em algum lugar do mundo com o mesmo endereço IP. Então, se houver um problema com alguma das duplicações, como vocês poderão diferenciá-los, considerando que eles têm o mesmo endereço IP? Como serão localizados? Obrigado.

FRED BAKER: Essa é uma pergunta sobre como funciona o Anycast, que era parte da discussão nas apresentações anteriores. O fundamental é o roteamento. Cada um desses servidores não apenas executa o serviço de resposta a solicitações, e aqui está a tradução, seja ela qual for, mas também interage com o BGP, com os ISPs ou os IXPs aos quais estão associados e anunciando seu endereço.

Então, quando uma solicitação vai de algum local até o endereço, o roteamento o direcionará à instância do servidor que estiver mais próximo topologicamente. Agora, se um dos servidores ficar inoperante, se o roteamento for perdido, caso algo de mal aconteça de alguma maneira, o endereço daquele local será retirado do BGP. O BGP não será mais roteado naquela direção e haverá outras instâncias que oferecerão o mesmo endereço. Então, o roteamento agora levará o pacote para algum outro lugar. Isso é apenas o modo como o roteamento funciona.

No pior dos casos, vamos imaginar — e não sei por que isso aconteceria, mas imagine que o endereço não estava mais disponível no roteamento. Simplesmente não existia. Uma das razões pelas quais temos 13 operadores de servidores raiz é para que o aplicativo que solicita isso, o resolvedor no computador de alguém, possa escolher um dos outros endereços e perguntar a outro. Portanto, há dois níveis de backup.

STEVE SHENG: Obrigado. Liman?

LARS-JOHAN LIMAN: Eu gostaria complementar que quando você usa o Anycast, cada servidor tem dois endereços IP. Um dos endereços IP é o mesmo para todos os computadores, sendo esse que é usado para o tráfego DNS. Além disso, cada servidor tem um endereço separado exclusivo. Ele é usado pelos operadores para alcançarem por trás, por assim dizer, para fazer o serviço e a administração.

STEVE SHENG: Obrigado. John?

JOHN CRAIN: Obrigado. Acho que você pergunta também como saber com qual deles você está se comunicando. Há realmente uma consulta de DNS para uma consulta TXT. Você precisa digitar CHAOS HOSTNAME.BIND e há algumas outras variações nas quais cada instância realmente tem um nome pelo qual você pode fazer uma consulta no DNS e que lhe informa qual é. Posso lhe mostrar isso no computador mais tarde, se você quiser.

STEVE SHENG: Obrigado pela pergunta e pela resposta abrangente. Senhor no fundo?

HOMEM NÃO IDENTIFICADO: [inaudível] da Índia. [inaudível] segurança [inaudível] DNSSEC. Você pode nos dizer em quais países as [DNSSEC] foram completamente implementadas e se ocorreu algum problema durante a implementação?

STEVE SHENG: Pergunta sobre a implementação das DNSSEC. Alguém? Acredito que há um workshop sobre as DNSSEC na quarta-feira. No começo desse workshop, eles mostrarão também os números da implementação em todo o mundo. Essa é uma sessão na qual você poderá se informar sobre esses números.

BRAD VERD: Isso está um pouco fora do escopo do RSSAC. Se houver uma maneira diferente de reformular sua pergunta e fazê-la atribuível à raiz, talvez possamos respondê-la.

KAVEH RANIBAR: Basicamente, apenas para esclarecer o que publicamos como operadores de servidores raiz, obtemos um arquivo de zona assinado. É a zona raiz que é assinada. Então, ela passou, o trabalho do RSSAC ou dos operadores de servidores raiz basicamente começa depois disso, quando já existe um arquivo de zona raiz assinado e basicamente distribuímos esse arquivo. Então, do nosso ponto de vista, apenas distribuímos uma zona raiz assinada e nos certificamos de que a integridade do arquivo que obtivemos seja mantida, e nos certificamos de mantê-la quando distribuímos o arquivo ou o conteúdo.

STEVE SHENG: Obrigado por isso. Mais alguma pergunta? O senhor ali?

TARAU BAUIA: Tarau Bauia, de Kiribati. Tenho uma pergunta. Quando implementamos as DNSSEC, há algum problema com os

subdomínios [ou digamos] em .com que não têm chaves ou que ainda não mudaram para as DNSSEC? Isso será um problema?

STEVE SHENG: Novamente, essa também é uma questão sobre as DNSSEC que se adequará melhor ao workshop de quarta-feira. Essa é minha visão. Portando, convido-os para esse workshop. Conversem comigo para saber mais detalhes sobre esse workshop. Agora, vamos passar para uma pergunta on-line e depois você é o próximo.

CATHY PETERSEN: Tenho outra pergunta on-line de Jose de la Cruz. A pergunta é: "Quem pode participar do RSSAC?"

STEVE SHENG: Obrigado.

BRAD VERD: O RSSAC tem uma Comissão que atualmente tem mais de 80 membros de especialistas no assunto. Todas as nossas equipes de trabalho vêm da Comissão, são patrocinadas por ela. Há — acho que está aqui na tela — a associação à Comissão. Se você estiver interessado, pode escrever para o endereço de e-mail. Temos um comitê de associação que analisa a inscrição. Você

precisa fornecer uma SOI, basicamente uma declaração de interesse. E então você faz parte da Comissão e da solução.

STEVE SHENG: Obrigado, Brad, e obrigado por essa pergunta Jose. Este senhor na frente?

HOMEM NÃO IDENTIFICADO: Steve? Posso?

STEVE SHENG: Sim, pode falar.

HOMEM NÃO IDENTIFICADO: Apenas para acrescentar que, apenas para reiterar, a maior parte do trabalho técnico real do RSSAC é feita por meio da Comissão. Então, se você for um membro da Comissão, basicamente você está fazendo o trabalho real. Assim, como você observou nos slides, as 12 organizações e os 13 operadores basicamente fazem a maior parte do trabalho de administração.

Quando recebemos uma pergunta ou quando é necessário um conselho, formamos uma equipe de trabalho na Comissão. E todos nós — os membros do comitê do RSSAC — também fazemos parte da Comissão do RSSAC. Então, se quisermos também fazer parte da solução, também nos juntaremos à

equipe de trabalho. Mas para cada pergunta ou conselho que recebemos, formamos uma equipe de trabalho e basicamente o trabalho é feito dentro da Comissão, então você fará parte desse RSSAC.

BRAD VERD: Acrescento ainda que o trabalho também pode ser atribuído às pessoas na Comissão que o executam. Então, não é a Comissão que faz o trabalho, escreve os artigos e outras pessoas recebem o crédito. Se você contribuir, receberá atribuição plena.

STEVE SHENG: Obrigado. Continue.

ABDULKARIM OLOYEDE: Certo, obrigado. Eu gostaria de saber a frequência das reuniões do RSSAC e da Comissão?

BRAD VERD: O RSSAC se encontra mensalmente. Temos teleconferências mensais nas quais são feitas minutas e as questões são abordadas. Essas teleconferências são públicas e podem ser — não?

HOMEM NÃO IDENTIFICADO: Apenas as minutas.

BRAD VERD: As minutas são públicas. Desculpe. As minutas são públicas. Além disso, o RSSAC se encontra aqui nas reuniões da ICANN e também no RSSAC. Nos últimos dois anos, realizamos dois workshops por ano, pois estamos fazendo um trabalho de evolução sobre o qual você poderá ouvir se comparecer à reunião pública do RSSAC aqui.

No que diz respeito à Comissão, ela funciona on-line. As equipes de trabalho acontecem o tempo todo. O trabalho nas equipes está em andamento, dependendo da própria equipe de trabalho. Pode haver teleconferências semanais ou quinzenais. Depende apenas da carga de trabalho que está realmente acontecendo.

As reuniões da Comissão ocorrem aqui na AGM. E isso é, a propósito, determinado pela Comissão. Então, a Comissão perguntou quando eles se encontrariam e chegaram à conclusão de que nos encontraríamos na reunião da AGM da ICANN, e nos encontramos em todas as outras reuniões da IETF. Acredito que a maneira mais fácil de dizer isso é que a Comissão realiza as reuniões nos IETFs de número par.

STEVE SHENG: Obrigado. E a próxima reunião da Comissão será no IETF 201, em Montreal. Obrigado. Mais alguma pergunta? O senhor à esquerda?

BONNIE MTENGWA: Certo, obrigado. Sou Bonnie Mtengwa da Telecoms Regulatory de Zimbábue. Tenho uma pergunta. Estamos interessados em ter um dos servidores raiz no Zimbábue. A ICANN auxilia os interessados em ter um servidor raiz ou isso depende do país que está negociando com os operadores de servidores raiz ou talvez haja ajuda da ICANN ou alguns requisitos que devam ser atendidos primeiro?

STEVE SHENG: Obrigado por essa pergunta sobre o interesse de hospedar uma instância de servidor raiz. Liman?

LARS-JOHAN LIMAN: Diversos, se não todos, mas pelo menos a maioria dos operadores de servidores raiz têm nuvens Anycast e estão dispostos a discutir sobre onde colocá-los e onde hospedá-los. Não se trata de uma discussão entre um país e um operador de servidor raiz, mas entre um host específico e uma organização de hospedagem. Muitas vezes, é um ponto de troca para o

tráfego da Internet ou é um grande provedor de serviços de Internet ou algo assim.

Você está certo em relação a haver certos requisitos que precisam ser atendidos, principalmente requisitos técnicos e financeiros. Estamos trabalhando na compilação de uma lista de pontos de contato, mas eu diria para você vir e conversar com algum operador de servidor raiz e tentaremos explicar como vemos o relacionamento e quais são os nossos requisitos e outros farão o mesmo de sua parte. Definitivamente, há espaço para ter um servidor [nome] raiz em seu ambiente, se pudermos encontrar uma maneira de atender aos requisitos, pois ele tem de funcionar, então há requisitos, sim.

STEVE SHENG: Obrigado, Liman. Mais alguma pergunta? O senhor na frente novamente.

ABDULKARIM OLOYEDE: Acabei de pensar que, sim, o DNS do servidor raiz é uma parte importante da Internet e o trabalho do RSSAC e dos operadores do servidor raiz parece ser muito aberto. Falamos sobre invasores tentando atacar os servidores raiz. Como vocês filtram isso? Quando uma pessoa tem um motivo oculto, considerando que qualquer um pode participar, qualquer um pode fazer parte

da reunião, qualquer um pode contribuir. Então, como isso é filtrado? Obrigado.

STEVE SHENG: Pergunta sobre como filtrar invasores [do trabalho no RSSAC].

KAVEH RANIBAR: Essa é uma boa pergunta, uma questão complexa [também] porque há várias facetas nisso. Porém, uma das coisas que penso, e estou falando apenas do RIPE NCC, mas acho que a maioria dos operadores de servidores raiz, se não todos, compartilham esse sentimento, de que não podemos garantir a segurança das raízes por meio da obscuridade. Portanto, somos muito abertos, não apenas em como trabalhamos, mas o DNS, por padrão, é aberto. Você pode obter muitas informações sobre instâncias, onde elas são hospedadas e tudo isso. Em muitos casos, nós publicamos, mas, mesmo que não o façamos, por meio do DNS com algum conhecimento básico, é fácil descobrir isso.

Então o sistema é aberto. Por meio do total de capacidade que temos do ponto de vista tecnológico, basicamente tentamos garantir a capacidade de responder a todas as consultas. E, sim, como operador de servidor raiz, também recebemos muitas, digamos, consultas não legítimas sem motivo ou por motivo de

ataque. Mas, no total, temos capacidade suficiente para [diferenciar] e ainda atender às consultas certas e às boas consultas.

STEVE SHENG: John?

JOHN CRAIN: Essas são redes executadas profissionalmente; portanto, todos os operadores têm engenheiros qualificados e pessoal de segurança e levamos a integridade de nossos sistemas muito a sério. É por isso que quando você hospeda uma instância, por exemplo, existem requisitos e alguns deles são sobre quem pode acessar as máquinas e como etc. Então, a segurança é algo que levamos muito a sério. Porém, como Kaveh acabou de dizer, o DNS, por padrão, e para atingir seu propósito, é muito aberto. Acho que é apenas a natureza do protocolo, por assim dizer.

STEVE SHENG: Obrigado. Brad?

BRAD VERD: Acho que vou pensar mais especificamente em sua pergunta. Eu acho que você estava falando sobre o RSSAC, o fato de a Comissão ser aberta e as pessoas sendo capazes de participar e

o que há lá para evitar que um invasor participe e tente fazer algo malicioso. Era esse o sentido de sua pergunta?

Sim, acredito que isso seja um risco. Nós queremos ser abertos. Queremos ser transparentes e ter os diversos pontos de vista das pessoas para que possamos encontrar a melhor solução possível para qualquer problema técnico que nos seja apresentado. Como copresidente, espero que haja verificações e ponderações suficientes em relação às pessoas que estão ali com boa intenção para que possamos identificar pessoas com más intenções e tentar trabalhar com elas para descobrir o que está acontecendo. Mas, até o momento, não estou ciente de que algo assim tenha acontecido, mas é um risco.

STEVE SHENG: Obrigado. Próxima pergunta? O senhor no fundo?

HOMEM NÃO IDENTIFICADO: Olá. Meu nome é [inaudível] e sou da Índia. Retorno a um ponto que você mencionou anteriormente em sua apresentação de que a rota de tráfego não é determinada pelo servidor raiz, mas pelos roteadores. Eu gostaria de perguntar a você, especialmente no que diz respeito ao fato que você apontou, os requisitos do RSSAC002 que são feitos aos operadores de servidores raiz para publicar suas estatísticas do servidor raiz.

Agora, se eu quiser determinar qual é o tráfego total da Internet originado de um determinado local ou fora de um país em particular, como posso extrapolar isso ou como posso medir isso a partir de algumas das estatísticas que estão prontamente disponíveis on-line e disponíveis em código aberto? Obrigado.

STEVE SHENG: [Obrigado pela pergunta].

BRAD VERD: Acho que a resposta curta é que você isso não é possível. O tráfego do DNS raiz não deve ser usado como medição do tráfego total da Internet.

HOMEM NÃO IDENTIFICADO: Não, desculpe-me por interrompê-lo, mas eu gostaria de perguntar também como faço [inaudível] uma espécie de estimativa ou aproximação, uma estimativa justa, como posso usar o tráfego do DNS como medição de atingir [inaudível]?

HOMEM NÃO IDENTIFICADO: Em geral, e o que Brad está dizendo, basicamente, até mesmo para ter uma estimativa útil, você não pode usar o DNS para isso. O DNS não é uma plataforma para isso, mas existem outras técnicas de medição. Por exemplo, se você quiser, procure o

Google MLAP. Com base no tráfego [torrent] exibido, eles tentam estimar o [restante do] tráfego de um país ou região.

Portanto, existem outros [produtos], mas o DNS não é a plataforma certa para isso. A principal razão para isso é que, em primeiro lugar, o conteúdo não passa pelo DNS. Mas a segunda parte é, o que você obtém no DNS em qualquer nível, especialmente na raiz, muito do que é armazenado em cache pelos resolvedores e a eficiência desse cache, não é visível para nós. Por isso, é basicamente impossível ter estimativas úteis, mesmo em relação ao tráfego de DNS, com base nisso.

HOMEM NÃO IDENTIFICADO: Permita-me acrescentar algo. Quando você consulta um sistema raiz e as estatísticas do RSSAC002 informam que tenho excesso de solicitações IPv6, muitos UDPs, muitos seja o que for, estão perguntando sobre solicitações feitas à raiz. São pessoas tentando encontrar .com e .net e assim por diante. Não estão procurando particularmente locais específicos ou empresas individuais. Eles estão buscando registros. Então, são os dados incorretos.

STEVE SHENG: Obrigado. Mais alguma pergunta? Temos alguma pergunta on-line?

CATHY PETERSEN: Nenhuma pergunta on-line.

ABDULKARIM OLOYEDE: Em termos do RSSAC e da organização da capacitação, vocês fazem algo assim? Capacitação para países em desenvolvimento ou pessoas interessadas? Porque, muitas vezes, se, por exemplo, eu estiver interessado, posso jamais trabalhar em um servidor raiz em minha vida, ou posso estar interessado no que vocês fazem e, algumas vezes, isso pode ser muito técnico para mim, pois não trabalho com isso no meu dia a dia, mas quero saber mais. Obrigado.

KAVEH RANIBAR: Darei meu ponto de vista, pois não sei se entendi direito a pergunta. Primeiro, permita-me agradecê-lo pela sua primeira participação como fellow. Muito obrigado por ser tão interativo. Isso é bastante incentivado.

Sobre a capacitação, na verdade, cada operador de raiz tem ou pode ter seu próprio plano. Por exemplo, estou falando no RIPE NCC. Somos um RIR, um registro regional da Internet, para a Europa, o Oriente Médio e a Ásia Central. Mas o que fazemos, não apenas em nossa região, mas também no resto do mundo, incluindo a África e a Região da AP, é trabalhar com outros RIRs.

Por exemplo, [inaudível] temos um MoU com AfriNIC para a África ou APNIC para a Ásia Pacífico e, especificamente, deixe-me usar o exemplo da África.

O que fazemos na África é que a AfriNIC formou uma aliança com a Sociedade da Internet na África e eles estão trazendo financiamento e conversando com operadores e com partes interessadas e nós realmente hospedamos alguns nós por meio desses fundos e dessa capacidade que foi construída por meio da Sociedade da Internet da África e [nosso RIR].

Portanto, essa é a metodologia que nós do RIPE NCC selecionamos. Outros têm diferentes métodos e maneiras de chegar às regiões. Então você tem de verificar cada operador de raiz.

E, apenas para mencionar, porque também havia uma questão sobre como obter instâncias de raiz, no site root-servers.org, você tem uma lista de cada operador e também o site deles para o serviço de raiz. Assim, você pode verificar o site do RIPE NCC para o serviço de raiz, o site da Verisign para o serviço de raiz. E lá você pode encontrar todas as informações. Por exemplo, nossos contratos com outros RIRs estão listados lá e a maneira como você pode acessar direta ou indiretamente por meio de [seu] registro regional da Internet está relacionada e mencionada ali.

HOMEM NÃO IDENTIFICADO: Se eu puder acrescentar algo, muitas dessas questões são operacionais por natureza e deve haver vários operadores de raiz aqui. Porém, eu gostaria de indicar novamente o estatuto do RSSAC sobre fornecer conselhos sobre o sistema de servidores raiz à diretoria e à comunidade. Muitas dessas questões não são realmente direcionadas ao RSSAC, e acredito que o grupo que está aqui teria prazer em respondê-las, e queremos ser o mais transparente possível, mas queremos continuar — há um delineamento entre os operadores de raiz e o RSSAC. Eu só queria detalhar isso.

STEVE SHENG: Obrigado por isso. Mais alguma pergunta? Dou-lhe uma. Ah, Liman.

LARS-JOHAN LIMAN: Só uma observação final. Se vocês tiverem perguntas após a sessão, por favor, venham e conversem comigo. Acho que o mesmo serve para o restante de nós. Estamos aqui por um motivo. Queremos conversar com vocês e ficarei feliz em dar as respostas que eu puder.

HOMEM NÃO IDENTIFICADO: Novamente, eu faria uma menção ao FAQ que foi recentemente adicionado à página do RSSAC na Web. Mesmo que, como afirmei anteriormente, muitas das perguntas que recebemos sejam de natureza operacional, nós nos esforçamos para registrar todas as perguntas que surgem em várias dessas apresentações, bem como perguntas que normalmente recebemos. Tratam-se de Perguntas Frequentes em constante evolução. Assim, se houver alguma dúvida sua que não esteja ali, tenho certeza de que outra pessoa pode ter a mesma pergunta. Então, compartilhe-a conosco e nós a adicionaremos às nossas Perguntas Frequentes e as tornaremos mais completas. Obrigado.

STEVE SHENG: Com isso, deixe-me mostrar na tela do site do RSSAC, temos reuniões, comissões, publicações e Perguntas Frequentes. Quando você clica no link, há muito mais informações sobre as minutas de reuniões, a afiliação na Comissão, todas as publicações do RSSAC e as perguntas frequentes.

O site root-servers.org, mencionado por Kaveh, é um gateway para servidores raiz individuais. Se vocês tiverem perguntas [opcionais] específicas, haverá informações de contato. Esse é também o local de onde, na apresentação, obtivemos o mapa

de Anycast. Você stambém podem buscar mais informações detalhadas nesse site.

Com isso, se não houver mais perguntas, agradeço sua participação e aos membros do RSSAC que responderam às suas perguntas. Obrigado. Esta sessão está encerrada.

CATHY PETERSEN: Obrigada a todos.

[FIM DA TRANSCRIÇÃO]