SAN JUAN – Sessão diária de Fellowship
Segunda-feira, 12 de março de 2018 – 12h às 13h30 AST
ICANN61 | San Juan, Porto Rico

PESSOA NÃO IDENTIFICADA: Vamos começar. ICANN 61. 12 de março. Sessão de bolsistas.

SIRANUSH VARDANYAN: Por favor, ali está o almoço. Então peço que tomem o almoço e venham para cá. Peço a todos os bolsistas que estejam perto, quero ver o rosto de todos.

Temos algum microfone móvel aqui? Temos microfone móvel ou não? Sim? Temos? Muito obrigado, Rachel. Agora trazem.

Ainda não estamos gravando, não é? Não estamos gravando? É sim que não estamos gravando, né?

A sessão diária do programa de bolsistas. Hoje temos uma sessão especial com os técnicos. Eles estarão a cargo dessa sessão. Estou muito bem acompanhada aqui. Queria passar a palavra para Rachel Reyes, e depois vou deixar que os outros façam a apresentação para que saibam quem estará aqui fazendo a apresentação.

Por favor, peguem o almoço, sentem aqui e prestem atenção, pois é uma sessão muito interessante. Rachel?

RACHEL REYES: Bem-vindos a essa sessão dos aspectos fundamentais do DNS para ver como funciona. Vamos ter uma sessão com 30 minutos depois para perguntas.

Sou Rachel Reyes, sou pessoal de apoio técnico para ICANN org. John Crain está aqui comigo a direita e vai ajudar com a parte de perguntas e respostas.

JOHN CRAIN: Oi, sou John Crain. Sou funcionário a cargo da ICANN para estabilidade, segurança e resiliência, e também trabalho nos serviços dos servidores raiz. Faz mais de 20 anos. Ali no telefone está Matt Larson, também conhecido como senhor DNS, que também está na indústria do DNS, certamente faz mais tempo que eu. Então passo a palavra novamente a Rachel.

RACHEL REYES: Muito bem. O que acontece aqui. Bom, vamos começar. Os endereços IP são fáceis de utilizar para as máquinas, isso é certo, é verdade. É para nós lembrarmos nomes, mas para nós é difícil lembrar números.

Por exemplo, vamos tomar alguns de nós, menos eu, tenho dificuldades para lembrar os números telefônicos da minha família e amigos. O mesmo acontece com os nomes e números que devemos lembrar geralmente.

Nos primeiros dias da internet os números eram muito simples, não haviam nomes de domínio. Eram nomes com uma só etiqueta, 24 caracteres no máximo, e eram o que chamamos de nomes host.

A resolução dos nomes tem a ver com mapear os nomes com endereços de IP. Nos primeiros dias de internet os arquivos host eram arquivos nomeados host.txt, e estavam monitorados pelo instituto de Stanford. Eram atualizados de forma manual através de correios eletrônicos, e isso se fazia conhecer uma vez por semana, e era descarregado através de FTP. Isso acontecia nos primeiros dias da internet.

O problema com esse sistema, é que tudo era editado de maneira manual. Portanto, era um sistema apto a erros e extremamente ineficiente, porque se deveria enviar um email antes de poder fazer atualização, e isso também requeria uma largura de banda significativa quando se tratava de carregar ou descarregar um arquivo. Isso não durou muito tempo.

Por isso, as pessoas começaram a conversar nos anos 80 sobre como substituir esse sistema atual. Chegaram ao que agora

conhecemos com o conceito de nomes de domínio, onde eram abordados as questões de escalabilidade desse sistema host.txt. E vocês podem encontrar mais informação nos RFC que estão mencionados aqui, o 799 e o 819 que vão contar mais sobre a discussão desse conceito do sistema de nomes de domínios DNS.

Em resumo vamos explicar o que é o DNS. Essa terminologia que utilizamos no sistema DNS. Temos DNS, o dado DNS, o resolutor e servidor de nomes, o guardado na memória cache.

E vou agora mostrar esse gráfico. Temos aqui o resolutor de aba que é o que vamos mencionar, e temos o servidor de nomes recursivos que envia consultas ao nosso servidor de nomes. Eles são os servidores que estão a minha esquerda e a sua direita. Esses servidores de nomes são aqueles que dão uma resposta definitiva a consulta que demandam os servidores recursivos, e damos uma pequena borbulha que fala de cache. A memória cache é utilizada no sistema DNS para que seja mais eficiente e escalável. Depois vamos aprofundar nesse tema mais para frente da apresentação.

O espaço dos nomes é a estrutura da base de dados de DNS que tem forma de árvore virada para baixo. Podemos olhar de cima para baixo, mas normalmente nonosso trabalho diário vemos diário para cima.

Então vamos tomar esse esquema. Não lemos .com.exemplo.www, dizemos www.example.com., que é o que nós denominamos um nome de domínio totalmente qualificado.

No espaço dos nomes, em primeiro lugar, temos a raiz. Esse é um nodo raiz, depois o que chamamos de nodos de primeiro, e depois do segundo e do terceiro.

Em cada um desses nodos há uma etiqueta. As etiquetas constam de caracteres legais que se podem utilizar, que são apenas o que chamamos em inglês de LDH, que corresponde as letras, dígitos e os hifens. Temos uma longitude máxima de 63 caracteres aqui. E podemos escrever .com tudo minúsculo, ou podemos colocar uma letra maiúscula e outras minúsculas. Em regra não interessa se vão usar maiúscula ou minúscula. Cada nodo tem um nome de domínio.

Então no nosso exemplo vamos utilizar essa árvore que aponta aqui na etiqueta, que está salientada, o nome de domínio www.example.com. Isso está tudo separado por pontos.

Como já disse, os nomes de domínio totalmente qualificados, FQDM, acabam com o ponto. A maior parte das vezes, quando estamos fazendo um nome de domínio não usamos esse ponto do final. Colocamos www.example.com e mais nada. Cada um é domínio do que está por baixo deles.

.com é um nodo superior do nosso domínio, e tudo que estiver abaixo disso corresponde ao território de .com, ou ao domínio de .com.

As zonas, as zonas são regiões administrativas, e cada zona se baseia nos limites de uma autoridade, que é delegada a uma entidade. Uma zona de DNS pode ter um domínio, ou muitos domínios, ou subdomínios.

A delegação cria zonas. Uma zona delegada é a principal, e as outras zonas criadas são as secundárias. Então, podemos ter aqui esse exemplo que é delegado a essa zona secundária, que é essa linha azul que podem ver no exemplo.

Os servidores de nomes, como disse antes, são os que respondem as consultas que estão pelos servidores recursivos. Os servidores de nomes autorizativos para uma zona tem conhecimento completo dessa zona. Então quando vocês enviam uma consulta a um servidor autorizativo vaziou para uma zona, porque essa zona tem que poder dar uma resposta a essa consulta. As zonas têm múltiplos servidores autorizativos, e isso é porque questões de redundância e eficiência.

Como se mantém os dados de uma zona sincronizados com diferentes servidores autorizativos? Temos um protocolo de DNS que está incorporado no servidor que faz a replicação da zona, e isso utiliza o servidor primário e outro secundário.

O servidor primário tem os dados das zonas definitivas, e se vocês querem fazer uma modificação nessa zona, isso tem que ser feito no servidor primário. Por outra parte, temos um servidor escravo, ou secundário. É ali onde se recuperam os dados de zona de outro servidor autorizativo, e processo através do qual se faz, se chama transferência de zona. A transferência de zona é a comunicação entre um servidor de DNS e outro autoritário.

Outro servidor que temos que mencionar aqui é o nosso, a partir do qual se origina o arquivo de zonas. Mas devemos lembrar que um servidor é mestre, não tem que ser servidor primário. O servidor secundário pode funcionar como primário, ou mestre também.

A transferência de zonas é iniciado pelo servidor secundário. E podem encontrar nesse RFC, por exemplo, 1996, que tem um mecanismo de como se faz essa transferência de zona, e como se fazem modificações ao arquivo de zona.

Agora podemos ver o registro de recursos de DNS. O registro de recursos de DNS é o que nós mencionamos como RR. Se vocês lembram do que eu disse antes, cada nodo tem um nome de domínio, e o nome de domínio tem diferentes tipos de dados vinculados. Esses dados, nome de domínio, são guardados nos RRs.

Temos diferentes tipos de registros de recursos, mas só vamos discutir alguns deles. Vamos passar a ver o formato desse registro de recursos. O registro de recursos conta com 5 campos, o dono TTL, classe, tipo, e depois RDATA. O dono é o nome de domínio com o qual se associa esse registro de recurso. O tempo durante o qual dura esse tempo, segundos que se podem guardar na memória cache, é um mecanismo para acessibilidade que muitas vezes não é utilizado. É o tipo de dado que guarda esse registro, e nossos dados RDATA são os dados que levam esse registro.

Se vocês olham para isso talvez resultem conhece-lo. Posso mostra-lo. Essa informação é o que chamamos de registros de recursos. Se vocês estão familiarizados com o trabalho em rede, vai estar a par do que eu estava dizendo. Vamos ver.

Aqui temos o tipo e RDATA, que sempre aparecem. Esses são os tipos de registros de recuros que mais comumente fazemos. A corresponde a um endereço IPv4. Se temos 4 As significa o endereço IPv6. NS o nome de servidor autoritativo. SOA o nome autoritativo que sempre aparece na zona. Então podemos encontrar a informação SOA no ponto. CNAME é um nome ou nome de outras áreas de domínio. MX é o servidor de troca de e-mails. PRT é um ponteiro que usamos para mapeamento.

Há muitos outros registros de recursos disponíveis desde dezembro de 2017, 84 tipos, e podem ingressar nesse website que está na tela para encontrar mais desses tipos de registros de recursos. Se vocês acessam essa página é isso que vão ver.

Então vamos ver A e os registros de AAAA. Esse é o formato que tem o registro A, vai dar um endereço de IPv4 e AAAA ao endereço de IPv6.

O servidor de nomes NS especifica o servidor de nome autoritativo para uma zona. Aparece em dois lugares. Na zona principal e secundária. Nesse exemplo a esquerda temos o nome da zona, e a direita o nome do servidor, não o endereço IP. E assim se fazem as delegações ou registros do principal secundário, do pai ao filho, e em .com temos 13 servidores de nomes. Basicamente essas são as 13 zonas raiz que temos.

Os registros nesse aparecem desde a raiz, até o nível de .com. E durante a delegação, também incluímos um registro de colado, que esse registro de colado é um registro de recurso de IPv4 e IPv6. E está incluído no registro principal como parte da delegação. Porque temos que ter esse registro de colado? Porque se estão fazendo uma consulta para o endereço de IP www.example.com tem que entrar pela zona raiz, e vai lhes dar o endereço IP de um servidor de nome, e vão dizer qual é o endereço IP de www.example.com. Vai olhar a raiz e não vai

encontrar a resposta porque não tem ainda o endereço de IP. Por isso que temos que ter um registro desses.

Ele é o início da autoridade SOA. Isso está localizado no ápice da zona, e aqui temos um exemplo e como se vê esse SOA. Temos o domínio, o servidor de nomes, o hostmaster.example.com, o administrador da zona. E depois o nome de série que é a versão atual do arquivo. Refresh significa quantidade de segundos que o servidor secundário tem que responder. Retry é a quantidade de segundos que o servidor secundário tem que esperar até tentar fazer uma transferência de zona que falhou. Expire é a quantidade de segundos que um servidor secundário pode receber os dados antes de fazer uma atualização, o mínimo é o TTL.

O CNAME cria um alias para um nome de domínio a outro. Então a direita, e suponho que a esquerda está CNAME, o alias CNAME a direita. Não, desculpem, a direita é o nome canônico, e do outro lado temos o alias. Gera um alias que nós chamamos de nome canônico, mas não gera em cadeias ou loops, porque não se vê bem nos dados.

O tipo de registro de troca de emails é um servidor MX, é um servidor. Por exemplo, no nosso exemplo que diz example.com, MX 10 mail.example.com. Então esses 10 e 20 números de correspondência corresponde com a priorização. Quanto mais

baixo for um número melhor é, porque essa é a forma que preferimos que seja encaminhado.

Mapeamento inverso, de certa forma, a maior parte das vezes estamos procurando o endereço de iP de um nome de domínio, mas as vezes temos que procurar um nome de espaço, e não no endereço. E é aí onde temos o registro que não resulta muito diferente, não usamos permanentemente, mas sim está dentro dos dados sempre. E dessa forma aparece. Desculpem, deixe eu ver.

Eu vou pedir a John Crain, porque temos in-addr.arpa.

JOHN CRAIN: Bom, porque dessa forma nós fazemos referencia a inversão e alguns protocolos verificam essa situação para ver se o nome está de acordo com o endereço.

RACHEL REYES: Aqui temos outro tipo de recurso, outros registros de recursos. Esses que aparecem aqui na tela fazem parte do DNS.

Esse é um exemplo de um arquivo de zona, por exemplo para example.com, temos o SOA, o nome do servidor, o IPv4, o IPv6, também o registro MX e o CNAME. Finalmente temos o registro

colado. Qual é o endereço de IP que eu disse, porque senão isso entra no loop.

Vamos agora ao processo de resolução. Como mencionei anteriormente, temos esses resolvedores, ou terminais, temos também os servidores de nomes recursivos, e esses são os que buscam os dados do DNS no espaço de nomes.

Esse resultado pode estar adapto em um telefone, o servidor de nomes recursivos são os que enviam as consultas aos servidores de maneira autoritativa, e os servidores são os que enviam a resposta.

Uma consulta de DNS sempre tem 3 parâmetros. Um nome de domínio, a classe e o tipo. E é o que aparece aqui na tela. Há 2 tipos de consultas, estão os resolutores finais que enviam as consultas, então os servidores não recursivos enviam consultas que não são recursivas, o que chamamos de derivações. Depois vamos falar disso. Eu vou pular esses slides.

Eu tenho que falar desse aqui. Vamos supor que vocês começam o processo de resolução e o servidor recursivo está vazio, um território desconhecido. Então vão diretamente aos servidores da zona raiz, porque o arquivo de zona raiz está aí.

Então como funciona, como encontram esses servidores raiz, e isso tem que ser configurado do servidor de nomes, e quem faz esse trabalho é o operador dos servidores.

Aqui temos a lista dos servidores de nomes raiz, e dos arquivos para encontrar a raiz. Esse é o nome do servidor, tem a ver com o IPv4, AAAA como o IPv6.

A administração da zona raiz, isso é muito complexo. Então não vamos falar disso, mas vamos manter tudo que é fácil aqui. Se querem saber alguma outra coisa eu acho que podem falar com Matt Larson e realmente se dão alguns M&M ele vai poder falar com vocês.

Há 2 organizações que são de administração da zona, ICANN e Verisign. Há 2 organizações que são as que operam os servidores autorizativos. Então o que vemos aqui é que Verisign tem 2 estabilizadores que são os servidores A e J. Porque tem 2 servidores? Mais uma vez John Crain e Matt Larson vão poder responder, mas acho que não falariam aqui, mas vão falar agora. Depois dessa sessão, a menos que John tenha tempo para contar toda a história.

JOHN CRAIN: Não. Tem a ver com a história. Uma vez que os nomes se distribuíram na década de 90, quando se distribuíram os nomes,

nem todos estavam organizados em organizações novas. 2 não tinham como se organizar, um deles foi a Verisign, com quem tinha uma boa relação com Jon Postel. E outro, o da L, ficou nesse lugar. Mas depois quando administrado pela ICANN isso mudou. Isso tem a ver com a história de distribuição, por isso a letra J foi para a Verisign.

RACHEL REYES: Se querem saber onde estão os servidores raiz de cada país, podem ir a esse lugar: root-servers.org, e posso apresentar aqui na tela.

Então digamos que queremos ver quais são os servidores raiz disponíveis em Porto Rico. Tá o L e o J, que estão disponíveis em Porto Rico nesse momento. Então podem acessar esse website se estão interessados nessa informação.

Também estão os Anycast que estão utilizando instâncias de servidores raiz que nos ajudam a buscar os servidores raiz do DNS mais próximo da localização em que cada um está. Também quando estão fazendo uma busca, se tem instâncias dentro do lugar geográfico onde estão é mais fácil encontra-las.

O processo de mudança da zona raiz, como já foi mencionado, essa é uma versão simplificada, porque há muito mais processos na verdade do que se mencionou aqui, não vamos analisar com

profundidade, mas apenas para que tenham uma ideia de como se modifica um arquivo da zona raiz. Começamos então por um administrador de TLDs, que pede a IANA que faça uma mudança. A IANA então vai implementar essa solicitação de mudança, vai atualizar a base de dados da zona raiz, e vai publicar a zona raiz para todos os servidores de zona raiz.

E agora vamos ver o que é o processo de resolução. Acontece o seguinte, sei que estão fazendo uma consulta no telefone, não tem que ser apenas no telefone, pode ser também em laptop, ou qualquer outro tipo de cliente. Digamos que temos um cliente que tem esse resolutor em estado terminal. Então vai se fazer uma pergunta de qual endereço de IP example.com. Essa pergunta passará ao servidor recursivo, com endereço de 4.2.2.2 e vai dizer qual é o endereço IP de www.example.com. Então esse servidor de nome recursivo vai responder. Eu não sei, mas talvez o servidor raiz tenha essa informação, porque o servidor de nome recursivo não tem essa informação ainda? É porque é novo, é um servidor totalmente novo.

Como já disse antes, está vazio. Então não tem tudo na memória cache. Então vai para o servidor raiz para localizar o endereço IP, porque o servidor raiz vai dar uma derivação, vai dizer “não sei o endereço, mas sei o endereço de .com”. Então o servidor de nome recursivo vai recorrer a esse servidor e vai perguntar qual é o endereço de IP de www.example.com.

O servidor de .com vai dizer “eu desconheço, mas sim, conheço qual o endereço IP do servidor de nomes example.com”. Então o servidor de nomes recursivo agora vai até example.com, e vai dar ao endereço IP, ou vai dar o endereço definitivo, ou final, e o servidor de nomes recursivos então vai dar o endereço de IP a esse resolutor terminal.

Isso acontece em segundos, não em minutos. Igual quando abrem um aplicativo da laptop no telefone, que as vezes leva um tempo a abrir a página do aplicativo. Mas estamos tentando de voltar a carrega-la novamente é muito mais fácil, porque? Porque a informação já ficou na memória cache do cliente.

Então a memória cache, obviamente, acelera o processo de resolução. Porque agora sabe qual é o nome, o endereço IP da zona raiz e dos servidores de nomes.

Então estão tentando acessar, ou se estão tentando de solicitar qual é o endereço IP de FTP.example.com, quando eu estou fazendo a pergunta de www.example.com agora está perguntando qual é o endereço de FTP.example.com. Então só vale o resolutor irá de novo aos servidores, mas dessa vez não vai voltar ao servidor da zona raiz, mas irá diretamente não a zona raiz, mas de forma direta ao servidor de nomes, porque já tem a memória cache.

Então, utilizando essa informação que tem em cache vai acelerar o processo com maior eficiência e mais rápido. Aqui está como acontece o processo de resolução, como funciona.

Eu acho que falta um flyer de DNSSEC, se querem entender bem o que são as sessões de segurança do DNS acho que há algumas sessões que vão falar desse tema de forma especifica. Há um essa semana da DNSSEC, podem participar.

JOHN CRAIN: Eu acho que quarta-feira há uma. Eu vou procurar e avisar antes de que acabe.

PESSOA NÃO IDENTIFICADA: Houve um tutorial ontem.

RACHEL REYES: Basicamente então esses são os pontos básicos da DNSSEC. Vou ler em voz alta. Podem assinar de forma digital para serem autenticados, cada zona tem algumas chaves públicas e privadas que funcionam, e há diferentes tipos de registros.

Por exemplo, esse aqui, que é chave publica com RRSIG, NSEC e NSEC3, que mostra um nome específico de uma área, e DS que é o assinante da delegação.

Se querem conhecer um pouco mais podem participar de uma dessas sessões do DNSSEC que acontecerão essa semana.

Bom falar então do ecossistema do nome de domínio que tem essa aparência. Temos o registro, que tem a data de base dos nomes de domínio e os registratários. O registrador que é o vínculo, e também temos o registratário, que é o titular da registração do nome de domínio.

Dessa forma se processam esses nomes de domínio, não vamos falar exatamente de como acontece isso, mas o que nós falamos tem a ver com o registro de nomes de domínio, e está tudo aqui. Os servidores autoritativos, os servidores recursivos e os usuários de internet.

E com isso termino a apresentação para a sessão de hoje. Não sei se há pergunas na sala.

JOHN CRAIN: DNSSEC quarta-feira das 9 da manhã até 3 da tarde. É o dia todo de DNSSEC, mais do que precisam todos.

SINARUSH VARDANYAN: Obrigado, vamos começar com as perguntas, por favor.

NICOLAS FIUMARELLI: Nicolas Fiumarelli do Uruguai. Vocês mencionaram que o DNS não está afetado, mas o que acontece com os nomes de domínio internacionalizados?

RACHEL REYES: Matt pode responder.

MATT LARSON: O DNS em si realmente não responde a caixa alta ou baixa. Os IDNs são uma camada por cima do DNS. Agora Rachel, poderia voltar as primeiras imagens que vimos? Aqui nas imagens podem ver o nodo onde a aparece na imagem da esquerda que quando implementamos por cima dessa situação, da perspectiva do usuário, se temos um aplicativo que permite usar os IDNs que se podem utilizar, os caracteres internacionalizados, esse aplicativo tem que converte-los nesse LDH que é o formato normal. Da perspectiva do DNS, vemos como uma coisa, por exemplo, uma coisa talvez engraçada. Isso se chama Punycode e tem base no Unicode, mas tem base nesses caracteres únicos para entrar no DNS.

NICOLAS FIUMARELLI: Obrigado.

MATT LARSON: Houve pessoas que quando fizemos isso disseram porque precisamos dessa camada por cima do DNS, porque não colocamos o UTF-8 e a etiqueta desse tipo dentro do DNS, mas houve uma preocupação, porque o sistema DNS não esperaria, não foi desenhado para agir assim. Então por isso deveríamos fazer uma atualização de toda a infraestrutura, e de todos os clientes, assim fizemos com os IDNs. Então temos todos os clientes no mesmo lugar, mas não temos que mexer no resto da infraestrutura do DNS.

Queremos tocar todos os aplicativos e a infraestrutura do DNS, ou apenas os aplicativos, por isso decidimos pela última opção.

SINARUSH VARDANYAN: Temos uma pergunta aqui.

ABDULKARIM OLOYEDE: Eu gostaria de fazer uma pergunta porque disseram que havia uma camada por cima do DNS. Ao mesmo tempo, do que eu entendo, isso significa que se envia uma consulta ao servidor DNS, enviam tudo ao servidor DNS. Então, como sabem, se essa camada está por cima do DNS? Antes de fazer a minha pergunta.

MATT LARSON: Quando falamos em uma camada por cima do DNS, ou nível por cima, é uma coisa de conceito, mas dentro de qualquer aplicativo que entenda os IDNs, por exemplo, no navegador que entenda os IDNs, podemos marcar caracteres não latinos, e vai converte-los em uma coisa que seja possível de ver. Como aparece aqui na tela, como acento // que pode ser ponto alguma outra coisa. Então uma etiqueta através de cada etiqueta que já está internacionalizada. Então esse navegador envia ao resolutor final, que envia por sua vez ao servidor de nomes, e essa consulta então é que tem acento // vai fazer dentro do aplicativo e não dos resolutores do DNS.

ABDULKARIM OLOYEDE: Apenas vou fazer duas perguntas. Quando se faz uma apresentação, não sei se eu perdi uma parte, ou se o senhor falou muito rápido, mas com respeito aos servidores da zona. O senhor falou que seria um pouco complicado, e eu estou um pouco complicado com esses servidores de zona. O que são servidores de zona? Especialmente quando falamos dos servidores de zona primários, secundários, alguns que podem funcionar como mestres e escravos. Pode explicar novamente isso? E com respeito ao 4.2.2.2 isso envia uma consulta. Isso é como ser recursivo por defeito para todas as consultas?

JOHN CRAIN: Se falamos os diferentes tipos de servidores de nome, porque estamos falando de servidores de zona, agora podemos voltar para trás nos slides. Basicamente há 3 grupos de servidores. Estão os servidores finais que estão na laptop ou no telefone, pode estar também no sistema operacional no aplicativo, como de buscador. E isso apenas responde em perguntas.

Depois estão os recursivos, que normalmente são manejados por um ISP, ou os senhores encontram dispositivos da casa. E esses passam os servidores utilitativos para buscar a resposta. E esses são serviços que têm a respostas. Então por isso falamos que são autorizativos, porque têm autoridade para dar a resposta. Aí está a resposta.

Agora no recursivo, há um motor de consulta que faz a consulta, e a única coisa que se guarda está no cache, que os resolutores terminais também podem ter esse sistema.

Então é uma trajetória que se acompanha do dispositivo para ser maior. E outro comentário que eu acho que foi feito por Rachel com respeito a complexidade de como se fornece o servidor raiz eu não sei se refere a isso. E isso é uma coisa totalmente diferente, é um sistema de provisionamento, mas não um sistema de servidores de nomes. Eu vou deixar a Matt que responda, porque ele trabalhou mais nessa área.

Mas, o que acontece com os servidores recursivos. Eles estão definidos quando o pessoal configura o computador, e aí você pode falar a rede vai para lá, então se utiliza um protocolo de configuração dinâmico do host, que diz que endereço de IP tem que utilizar, e também os servidores recursivos dos nomes de domínio. Podem ter 2, ou 1, ou 4 deles. E todas as consultas depois iriam a esses que estão configurados.

SINARUSH VARDANYAN: Há uma pergunta de participante remoto.

MATT LARSON: 4.2.2.2 de comunicações em ISP. É um servidor recursivo aberto, e em qualquer lugar há vários clientes. Tem uma rede para clientes de banda larga, ou nesse prédio que nós estamos, um resolvedor a esquerda abaixo. Nós estamos em um servidor recursivo.

E como disse John, quando você se conecta a rede, você entra no número de IP para se auto configurar. E se não houver vocês podem usar outros servidores abertos recursivos que são públicos, de terceiros, e talvez o mais comum é o DNS público Google 8.8.8.8. Você pode configurar no seu telefone para que ele vá para esse endereço.

Outros são o DNS aberto, foram os primeiros a dizer vamos utilizar os servidores recursivos fora da sua rede, e vemos oferecer esse serviço a Verisign, a PCH também. Há vários públicos. E 4.2.2.2 é do Level 3, que já existe há bastante tempo.

SINARUSH VARDANYAN: Obrigado. Há uma pergunta de um participante remoto da África. “A África parece estar se desenvolvendo gradualmente e precisa aumentar sua capacidade. Além do programa de fellowship, o que o DNSSEC está fazendo para aumentar a sua capacidade? E o que está fazendo na África em termos de políticas?”

JOHN CRAIN: A questão da capacitação, não estamos falando do DNS, capacitação em relação a um DNS. Em geral trabalhamos com a comunidade. O meu grupo especificamente faz muita capacitação, treinamento, mas na África especificamente, há organizações como AfriNIC, AFNOG, AfTLD (domínio de topo da África), eles fazem esse tipo de treinamento, nós trabalhamos com eles, damos suporte.

Tem um centro de recursos de startup na África que ensina sobre o DNS e estruturas de infraestrutura.

E quanto ao DNS especificamente, nós realizamos vários treinamentos na África com a AFNOG, e todas as organizações da África. Eu não sei quando será o próximo, mas eu acho que haverá treinamento de DNSSEC programados para a África. Eu acho que em maio ou junho.

Temos sido bastante ativos, e dependemos dos especialistas locais. E tentamos treinar o mundo, que é muito grande, esse não é a tarefa da ICANN. A ICANN é uma organização pequena. Alguns acham que é muito grande, mas na verdade é pequena. Nós precisamos envolver as comunidade técnicas locais e ajuda-los a desenvolver os seus materiais, e capacita-los.

Estamos trabalhando com plataforma de aprendizado online, e queremos também fornecer mais e-learning, ou aprendizado eletrônico, traduzir materiais também.

Embora não sejamos uma universidade, passamos muito tempo treinando pessoas. Se olhar o título de segurança, resiliência e estabilidade, uma das coisas é garantir que as pessoas possam construir sistema melhores.

SINARUSH VARDANYAN: Obrigado.

LENDON TELESFORD: Lendon de Granada. Eu não sei se é uma pergunta do DNS em si. Bom, eu vou perguntar de qualquer forma. Na apresentação foi destacado as diferentes instancias dos servidores raiz. A minha pergunta é: o servidor cliente, quais são os mecanismos para proteção ao DDoS, que pode fazer com que o cliente se confunda sobre qual servidor acessar.

MATT LARSON: Bem, eu não sei o que você quer dizer com os clientes se tornarem confusos com um servidor raiz. Eu vou usar o conceito novamente de camada. O Anycast é uma camada abaixo do DNS. Então temos o DNS, o Anycast é para o sistema de roteamento da internet.

Então o sistema de servidor raiz, cada um dos endereços de IP está no Anycast. Então vai ser enviado uma consulta pela raiz R. Então o que está dizendo, vou mandar uma consulta para esse endereço de IP. Então o Anycast tem que transportar esse pacote, e os roteadores vão ver que há várias instâncias, vários locais na rede em que há vários endereços de iP.

Então diferentes redes anunciam a rota para cada rede. Roteadores individuais usando o BGP. Eles vêm qual é a melhor forma para chegar a raiz L. Então eu quero mandar um pacote para a rede L, então você vai para o local mais próximo, não é geográfico, não é uma questão só de latência.

Eu não tenho certeza de onde é que a confusão entra aqui. Se houver um ataque em um local, houver uma sobrecarga, então quando o servidor de nomes diz assim “eu estou aqui e podem anunciar que a minha rota existe” mas se isso se tornar tão congestionado que cair, então dependendo da falha ele vai dizer para a rede “bom, eu não estou mais ao vivo” então a rede recalcula, e vai enviar esse tráfego para outro lugar.

LENDON TELESFORD: As decisões sobre qual roteador, ou qual rota, já estão estabelecidas no BGP?

MATT LARSON: Eu diria que não muda a todo o tempo. Cada sistema autônomo, como dizemos, o sistema BGP tem várias rotas, várias redes para as quais anuncia.

Então cada roteador BGP são essas redes que conheço. Há outras rotas ou roteadores. Na verdade é uma versão muito simplificado do que acontece na verdade. O BGP é o que faz isso.

JOHN CRAIN: Isso não é causado necessariamente por Anycast. E isso acontecia antes do Anycast.

Há vários caminhos até os nodos. Então se eu estiver muito fora, se eu estiver próximo eu vejo várias rotas. Então é questão de um truque de roteamento que foi identificado e usado para adicionar mais servidores. Não houve mudança de tecnologia do Anycast, é só uma mudança de roteamento.

LENDON TELESFORD: Eu acho que minha pergunta tenha a ver com isso.

JOHN CRAIN: Eu não ahco que isso é parte do truque. O roteamento tem problemas de segurança, mas não tem a ver com Anycast. Na verdade o que se deve dizer é falta de segurança, mas isso não é específico do Anycast.

SIRANUSH VARDANYAN: Obrigado.

SHABNIL ANAL SAMI: Se um país quiser hospedar um servidor raiz, quando isso é decidido, isso é baseado em região?

JOHN CRAIN: Depende com quem você vai falar, não depende de um país, mas de um operador de rede, ou de uma rede, ou de um

operador de rede que quer hospedar um servidor. Então temos uma lista de operadores, nós somos um dos operadores. Eu acho que há um em Fiji. Então você pode fazer contato com esses operadores, quais são as suas condições para isso, e eles operam de forma levemente diferente.

Há vários locais ou instâncias hoje. Então acrescentar mais é só entrar no site e há links para cada um dos operadores, e há documentações de como contata-los. Eu posso falar com você depois para ver isso.

SHABNIL ANAL SAMI: Eu queria saber qual L, F. Porque em Porto Rico ele está hospedando L, Fiji, outro. Não é uma questão regional, é mais uma questão de relacionamento.

JOHN CRAIN: Há razão porque Fiji tem L. Porque nós temos um funcionário em Fiji. Muitas vezes tem mais a ver com relacionamento. Você vai no site e diz “bom, esse parece ser legal” e também os critérios, geralmente financeiros, são diferentes.

Nós na ICANN temos uma solução, você paga pelo servidor, você coloca online e nós fazemos o trabalho. Outros você envia o dinheiro e eles enviam os servidores. As raízes L são iguais e dão

as mesmas respostas. Funcionam do ponto de vista de consulta, exatamente igual. Depende mais de quem você conhece.

SIRANUSH VARDANYAN: Mais alguma pergunta?

PESSOA NÃO IDENTIFICADA: Eu tenho 2 perguntas. Como garantir a publicação das áreas dos registros dos países? E a segunda pergunta, as cópias das rotas das raízes, dos servidores raiz, são parte das zonas de todo o mundo? Na raiz L, por exemplo, é parte de todas as zonas ou todos os registros estão aí?

MATT LARSON: Todas as raízes, há apenas uma zona raiz com as informações, e todos os servidores raiz tem a mesma informação.

Você poderia repetir a primeira pergunta?

SINARUSH VARDANYAN: Há tradução, você pode fazer no seu próprio idioma. Aproveite esta oportunidade.

PESSOA NÃO IDENTFICADA: Quando os registros de cada país fazem um registro da zona, um ccTLD ou qualquer outro, e isso é publicado para o distribuidor

de toda a zona do DNS. Como garantir que essa publicação seja correta e que não haja erros. Ou na distribuição, como eu soube que já ocorreu.

JOHN CRAIN: Há algumas perguntas então. Há uma mistura de terminologia e tecnologia. Em relação ao ccTLD ou gTLDs. Quando publicam a zona, essa zona é composta de dados que vêm da base de dados, e são responsáveis por garantir que esses dados são corretos, e depois de publicados, se o DNSSEC assinar a zona e você autenticar as consultas do DNS, você pode garantir o que foi publicado.

Essa é a parte final. Essa é a publicação do lado do DNS. O outro lado disso tem a ver com a segurança de base de dados da rede, integridade dos dados. Houve problemas no passado em que fizeram hack dos sistema de ccTLDs.

Não existe nenhuma rede verdadeiramente segura. Eu acho que as pessoas estarão sempre suscetíveis de certa forma, e o que nós fazemos na ICANN e com os amigos nos registros, e eu especialmente no meu grupo de segurança, quando eles têm problemas, eles fazem contato conosco, e nós os ajudamos com a recuperação, e também para encontrar especialistas para reprojetar os seus sistemas.

Eu acho que sei o que você está se referindo, mas eu não vou dizer o nome aqui. Em alguns casos que houve ataque de SQL. O que permite que o violador mude os registros de uma grande organização, e direcione o servidor para outro lugar.

Então parece que o servidor foi atacado, mas não foi isso. Foi o registro na verdade. E nós temos trabalhado com operadores que têm um sistema totalmente novo, e tem maior proteção. Aprenderam com os seus erros e progrediram.

Então isso é o que acontece no caso quando há um problema. Você aprende o que aconteceu, concerta o que precisa ser feito e se protege. Um gTLD nunca é atacado, grandes corporações são atacadas também.

PESSOA NÃO IDENTIFICADA: Muito obrigado.

SIRANUSH VARDANYAN: Seu nome, por favor.

JASON HYNDS: Jason Hynds de Barbados. A minha pergunta é então, há alguma publicação feita para ajudar os operadores de registro a prevenir esse problemas antes que eles aconteçam?

JOHN CRAIN: Trabalhando com os parceiros que eu falei antes em termos de capacitação, fizemos milhares de horas de treinamento com operadores. Como monitorar uma rede, como garantir a segurança, mas é claro que a comunidade, que você vê aqui de operadores, também tem seus próprios grupos, compartilham muitas melhores práticas, e também suporte de engenharia. A Jamaica é parte da região da LAC, existe a LACTLD que reúne a maior parte dos registros da região, e se reúnem regularmente.

E uma das coisas é ajuda-los. Não é algo que eles tenham que enfrentar sozinhos, mas isso deve ser feito por toda a comunidade. Há treinamento e há ajuda uns dos outros.

SINARUSH VARDANYAN: Alguma pergunta? Não há mais perguntas?

Muito bom, então incentivo que participem na oficina de DNSSEC na quarta-feira das 9 da manhã as 3 da tarde.

PESSOA NÃO IDENTIFICADA: É longo.

SINARUSH VARDANYAN: No meio vamos ter sessão de almoço dos bolsistas. Mas eu acho que é uma oficina importante. Alguma outra coisa daqueles que fizeram as apresentações?

RACHEL REYES: Muito obrigado. Obrigado John e Matt por ajudar a responder as perguntas.

SIRANUSH VARDANYAN: Obrigado aos intérpretes e a equipe técnica. Realmente muito brigado a Matt, John e Rachel pelo tempo. Eu sei que nessa reunião estão muito atarefados, e eu agradeço muito a presença para que os bolsistas recebam esta apresentação.

Sem mais, encerramos a sessão, obrigado.