ICANN (Corporação da Internet para Atribuição de Nomes e Números)

Painel de Inovação da Tecnologia de Identificadores — Relatório Preliminar

21 de fevereiro de 2014

Sumário

1. Introdução

O painel de ITI (Identifier Technology Innovation, Inovação da Tecnologia de Identificadores) foi formado pela ICANN (Corporação da Internet para Atribuição de Nomes e Números) com os seguintes objetivos:

1. Desenvolver um roteiro de tecnologia para o DNS (Sistema de Nomes de Domínio) e outros identificadores

2. Desenvolver recomendações de melhores práticas e sistemas de referência

3. Fornecer orientação tecnológica para operações, segurança, política e funções técnicas da ICANN

4. Manter contato com a comunidade da ICANN e o público sobre assuntos de tecnologia

O painel foi selecionado em setembro e outubro de 2013, com Paul Mockapetris como presidente. Todos os membros participam por conta própria, e suas afiliações servem apenas para fins de identificação:

- Jari Arkko — presidente, IETF (Força-tarefa de Engenharia da Internet)
- Rick Boivie — IBM Thomas J. Watson Research Center
- Anne-Marie Eklund-Löwinder — gerente de segurança, Internet Infrastructure Foundation
- Geoff Huston — cientista-chefe, Asia-Pacific Network Information Center
- James Seng — CEO, Zodiac Holdings
- Paul Vixie — CEO, Farsight Security
- Lixia Zhang — presidente Postel em Ciência da Computação, Universidade da Califórnia, Los Angeles

Foram realizados encontros presenciais no IETF (Força-tarefa de Engenharia da Internet) de Vancouver (novembro de 2013), no encontro da ICANN em Buenos Aires (novembro de 2013) e no escritório da ICANN em Los Angeles (janeiro de 2014). O Encontro de Buenos Aires foi aberto ao público, e um resumo das atividades do painel também foi apresentado por meio de dois seminários na Web em janeiro de 2014. Discussões eletrônicas por e-mail, entre outros, serviram de complementos. O relatório estará disponível para comentário público em fevereiro de 2014 e será finalizado no encontro de março da IETF em Londres.

O presidente gostaria de agradecer ao painel por todas as suas contribuições e ideias, e à ICANN por dar apoio ao painel. Agradecemos também Elise Gerich e Alice Jansen da ICANN, que contribuíram com ideias e apoio para todo o trabalho do painel.

2. Estratégia do painel

O nome do painel não é por acaso. O escopo foi ampliado, ultrapassando os limites propriamente ditos do DNS, em reconhecimento ao aumento da importância dada aos identificadores de todos os tipos para a Internet, bem como à função da ICANN no gerenciamento de outros identificadores. Uma lista parcial do atual portfólio da ICANN inclui:

- Nome de domínio
- Números de sistemas autônomos
- Endereços IPv4 da Internet
- Endereços IPv6 da Internet
- Endereços multicast
- Números de portas
- Números de protocolo
- Registro de URI (Uniform Resource Identifier, Identificador Uniforme de Recursos)
- MIB (Management Information Base, Base de Informações de Gerenciamento)
- Banco de dados de fuso horário

No entanto, em paralelo a essa ampliação, o cronograma do painel foi reduzido de originalmente um ano para aproximadamente seis meses. Isso resultou em um foco mais voltado para DNS do que o esperado.

Para compensar, o painel adotou os seguintes princípios:

- Tentar documentar todas as ideias consideradas, mas concentrar-se em algumas
- Buscar tendências impulsionadoras em particular (por exemplo, a expansão da Internet, tendências na arquitetura de processadores)
- Buscar as necessidades imediatas
- Evitar concentrar-se em assuntos bastante discutidos (por exemplo, implementação de DNSSEC, estratégias existentes para colisões) e buscar ideias inovadoras

A finalidade central do painel é informar o processo de planejamento estratégico da ICANN. Embora o painel tenha considerado ideias relacionadas com as necessidades operacionais da ICANN, ele não se deteve somente a ideias que seriam implementadas pela ICANN. A implementação de muitas das ideias discutidas no presente relatório ficaria naturalmente a cargo da IETF ou de outro grupo. Algumas das ideias levantam questões referentes a políticas. Essas questões não foram abordadas, a não ser para indicá-las.

Por fim, considerando o volume intenso de atividades no espaço de identificadores, o painel simplesmente realizou uma amostragem desse espaço. O leitor não deve supor que tínhamos o conhecimento de todas as atividades, nem que as ideias não mencionadas neste relatório são menos importantes.

3. Roteiro

Os identificadores são um tópico popular na comunidade da Internet. Em pouco tempo, os novos TLDs (Top-Level Domains, Domínios de Primeiro Nível) serão colocados on-line. Sua conta no Facebook deverá se tornar sua credencial de Single Sign-On para a Internet, assim como sua conta do Google. A longo prazo, a comunidade de pesquisa tem muitos projetos diferentes, inclusive o CCN (Content Centric Networking, Sistema de Redes Centrado em Conteúdo), o ICN (Information Centric Networking, Sistema de Redes Centrado em Informações), o NDN (Named Data Networking, Sistema de Redes de Dados Nomeados), entre outras variantes. Embora não consigam concordar em um nome para o campo, todos estão de acordo que o conteúdo deverá ser identificado pelo nome, o local do nó e que o cache deverá ser oportunista. Outras propostas insistiram que nomes simples (flat names) são a onda do futuro, e que nomes autocertificadores (self-certifying names) devem ser a base para qualquer novo sistema.

Os identificadores são centrais para qualquer rede no que diz respeito à identificação exclusiva de componentes da rede para todos os outros componentes da rede. Além disso, as redes modernas não são um domínio único homogêneo, mas sim construídas como uma amálgama de várias tecnologias, e há um requisito para mapear entre os reinos da identidade. Essa função de mapeamento é realizada de diversas maneiras. No contexto da Internet, um dos reinos de identidade mais visíveis é o reino do nome de domínio, que é um espaço de nome estruturado hierarquicamente. Há uma função de mapeamento associada a esse espaço de nome que pode mapear de nomes de domínio para outras identidades (como endereços IP, por exemplo). Quando observamos um roteiro para identificadores precisamos estar cientes da distinção entre o reino do identificador e a função de mapeamento, e buscar cada um deles no roteiro.

Na Internet atual, o painel identificou diversos fatores que têm a tendência de expandir o uso do DNS, bem como diversos deles que servirão para contrai-lo. Esses fatores não são todos técnicos, e o esforço pareceu mais darwiniano do que baseado em elegância ou alguma outra virtude.

Atuais fatores de expansão

- O DNS desfruta de uma vantagem herdada: ele é implementado em cada dispositivo que tocar a Internet. O simples crescimento da base existente expandirá o seu uso. Por exemplo, um aplicativo que quiser passar por firewalls e ser colocado em cache na Internet encontrará o DNS como uma base existente.
- Os novos TLDs tentarão monetizar suas marcas. Apesar de haver muitos céticos na comunidade técnica, mais de mil novas marcas estarão se empenhando para prosperar, e provavelmente teremos inovação e diversas surpresas.
- Novos recursos emergentes, como os recursos de segurança de DNSSEC (Domain Name System Security Extensions, Extensões de Segurança do Sistema de Nomes de Domínio) ou a DANE (DNS-based Authentication of Named Entities, Autenticação Baseada em DNS de Entidades Nomeadas), poderão motivar ainda mais o uso.

- Novos dados no DNS podem expandir o seu uso, especialmente quando combinados ao DNSSEC para garantir autenticidade. Um painelista defendeu a publicação do "aniversário" e da "atividade" de domínios como informações básicas de reputação. Outras propostas usaram o DNS como um registro de blocos de endereços etc. A ICANN restringiu o uso de alguns rótulos em nomes de domínio, e um registro em tempo real deles poderá ser apropriado, particularmente quando especificações impressas vierem em vários alfabetos.

Atuais fatores de contração

- O DNS é o padrão herdado, mas isso também é uma desvantagem, pois a lógica integrada do DNS nos pontos de acesso de Wi-Fi, modems DSL (Digital Subscriber Line, Linha de Assinante Digital) e cabo, firewalls, roteadores e a base de software da Internet frequentemente limita o escopo de uso e restringe a inovação. As implementações geralmente não são completas, atualizadas, nem estão em conformidade com os padrões. Essas questões atrapalharam a implementação de DNSSEC e tornam problemática a implementação de quaisquer recursos ou tipos de dados de DNS novos. Isso resulta em práticas de projeto como, por exemplo, limitar todo o uso de registros de texto (TXT) e endereço. Essa ossificação não é exclusiva ao DNS.
- Há um interesse comercial em estar no controle ("ser proprietário") da janela de pesquisa e/ou do espaço de identificadores. O interesse aqui é ver a intenção do usuário em sua forma livre e mantê-la escondida da Internet aberta. Observamos a tendência em dispositivos cujos códigos são fixados em um serviço de DNS específico, bem como em extensões de propriedade particular, representando um caminho para a balcanização.
- Os usuários preferem uma interface mais avançada. Em vez de digitarem os nomes do DNS, os usuários e os aplicativos geralmente utilizam a pesquisa e outros mecanismos para obter determinadas informações. A barra de URL (Uniform Resource Locator, Localizador Uniforme de Recursos) nos navegadores, por exemplo, é amplamente usada como uma ferramenta de pesquisa hoje em dia. A atual interface do usuário é o dispositivo móvel, que não favorece a digitação. O reconhecimento de voz e outros tipos de AI (Artificial Intelligence, Inteligência Artificial) na barra do navegador resultam em incompatibilidades entre os diferentes fornecedores. Como um exemplo, uma experiência de Geoff Huston (consulte a seção de contribuições) observou a pesquisa iniciada por "Geoff.Huston" em vários navegadores e não notou basicamente NENHUMA consistência entre os fornecedores. Essa falta de consistência pode ser tolerável em uma pesquisa de navegador em que o usuário deverá analisar os resultados, mas pode ser perigosa em arquivos de configuração de sistemas — uma das preocupações são as colisões.

A sensação do painel foi que, embora o uso do DNS possa desaparecer da interface do usuário, é provável que permaneça como uma ferramenta da infraestrutura. Uma analogia foi que o DNS não é como o papel enfrentando o ataque de eBooks, mas sim como um conjunto de instruções de computadores acessado por meio de linguagens de nível superior.

As opiniões diferem no que diz respeito a se seria possível ou aconselhável buscar um renascimento ou uma reestruturação do DNS. A tecnologia é discutida na seção "Fundamentos do DNS" deste relatório.

Há a questão política referente a se a ICANN deveria tentar preservar e ampliar o sistema de DNS. Se for o caso, como seria possível obter uma arquitetura consistente com base nos diversos pontos de vista do grupo constituinte da ICANN, da IETF (onde o trabalho presumivelmente seria realizado) e de outras partes na Internet?

O longo prazo

Um conjunto de ideias a longo prazo é o modelo de NDN (Named Data Networking, Sistema de Redes de Dados Nomeados). Suas principais ideias são o acesso de conteúdo por nome, autenticação digital em todos os lugares, cache oportunista e um esquema de fluxo no qual as solicitações de conteúdo e as respostas seguem o mesmo caminho. O modelo para o roteamento de consultas é, às vezes, representado como simplesmente usar uma hierarquia de nomes para decisões de roteamento por correspondência de prefixo mais longo, e é considerado pelos céticos como não dimensionável. De qualquer forma, áreas de teste de software, hardware e de várias redes são implementadas. Os aplicativos mais óbvios são para a distribuição de conteúdo, mas os defensores alegam que o modelo é bom para o controle de processos, redes automotivas etc.

De certa forma, o DNS foi a primeira das alternativas já esboçadas ao ICN puro, assim como abordagens mais atuais [Fayazbakhsh 2013] que tentam preservar somente as partes mais importantes do modelo de ICN. Importância aqui está aos olhos de quem vê.

O DNS recupera dados pelo nome. Ele não tenta fazer o roteamento por nome e, em vez disso, usa a camada de endereçamento da Internet; esse esquema corrige o que alguns consideram o principal problema de dimensionamento do ICN. De certa forma, o DNS ganhou a má reputação de ser um veículo para o tunelamento de vídeo [Kaminsky 2004] e o tunelamento ilícito de acesso por meio de consultas ao DNS realizadas antes da autenticação por alguns pontos de acesso Wi-Fi. (A pesquisa “DNS tunneling” [“tunelamento de DNS”] no Google retorna cerca de 1.620.000 resultados.)

O ICN tem uma correspondência de prefixos mais longos e seletores, o que permite a transferência de mídias, facilidades que foram antecipadas na seção de consulta da especificação original do protocolo de DNS, mas que nunca foram desenvolvidas.

De qualquer forma, supondo que seria possível aumentar os pacotes de DNS e adicionar alguns campos de consulta, os serviços de conteúdo poderiam ser replicados no DNS. A correspondência de respostas e solicitações autenticadas do ICN podem ser a melhor maneira de evitar os ataques de amplificação do DNS.

Concluindo, seria possível imaginar um esquema de NDN para substituir o DNS, provavelmente começando por um superconjunto das facilidades do DNS em uma transição que poderia levar anos ou décadas para ser finalizada. Qualquer tentativa para melhorar a arquitetura do DNS poderá se basear livremente no NDN.

O ICN não é, de maneira nenhuma, o único modelo para o futuro, mas sim o mais desenvolvido. Acreditamos que é sempre importante tentar abstrair os princípios básicos e, depois, estudar a

composição. [Ghodsi 2011] é um bom exemplo uma vez que relaciona a trindade nome, ID do mundo real e PKI (Public Key Infrastructure, Infraestrutura de Chaves Públicas).

Mais recentemente, veio à tona uma ênfase na distribuição de controle [Newyorker 2014] e privacidade, sendo que o sistema Namecoin é o exemplo mais conhecido. A PKI que existe representa um recurso para a vigilância em grande escala e, assim, um problema para a privacidade. Uma mistura de objetos autocertificadores e uma PKI opcional, ou talvez PKIs paralelas ou sistemas Peer to Peer (P2P), seria a resposta.

4. Problemas operacionais

Vários problemas aparecem nas operações diárias da ICANN. A maioria deles está relacionada à raiz.

4.1.Fortalecendo a raiz

Considerando a importância central da infraestrutura da raiz, o painel analisou várias sugestões externas de tecnologia computacional confiável. O painel achou que é possível haver algum mérito para esse tipo de tecnologia nos sistemas usados para editar e assinar a raiz, mas considerou que melhorar a distribuição de dados assinados por hardware comum era uma prioridade melhor para o painel. As revelações Snowden levantam algumas preocupações com a segurança de hardware que podem não ter sido consideradas durante o projeto dos sistemas atuais, como infecções de BIOS, spyware de disco rígido, entre outras [Spiegel 2014].

4.2.Replicação

O DNS sempre teve dois mecanismos complementares para a distribuição de dados: replicação pré-planejada de zonas e consultas sob demanda. Do ponto de vista de uma peça individual dos dados de DNS, um registro de recurso (RR), ela começa em sua origem definitiva como parte de uma zona, se movimenta com essa zona em uma ou mais transferências de zonas e, em seguida, termina sua jornada para seu destino definitivo quando é retirada por meio de uma consulta.

Por exemplo, a zona raiz é gerada pela ICANN em parceria com a Verisign e o Departamento de Comércio dos EUA, e depois distribuída para todos os servidores raiz pelas transferências de zonas. Conceitualmente, essa distribuição, assim como a distribuição de qualquer outra zona no DNS, pode ser feita por qualquer mecanismo: entregas de fitas magnéticas e pela Federal Express (FEDEX), transferências de arquivos pelo FTP (File Transfer Protocol, Protocolo de Transferência de Arquivos) ou Rsynch, ou, o que seria ideal, por uma transferência de zonas incremental que envia alterações de uma versão anterior, em vez de toda a zona. As cópias podem ser enviadas pela notificação do DNS ou recebidas por meio de uma estratégia de pesquisa que busca alterações. A segurança das transferências de zonas podem ser realizadas pela TSIG (Transaction Signature, Assinatura de Transação) do DNS e/ou

por vários outros protocolos de transporte, por exemplo, IPSEC (Internet Protocol Security, Segurança de Protocolo de Internet), HTTPS (Hypertext Transfer Protocol Secure, Protocolo de Transferência de Hipertexto Seguro) etc. Existem centenas de instâncias de servidores raiz com cópias da zona raiz.

Quando os usuários querem acessar dados na zona raiz, eles enviam consultas para a raiz. O roteamento das consultas é feito por dois mecanismos: primeiro, o endereço IP de destino na consulta identifica um conjunto de servidores raiz que compartilham um endereço anycast em comum e, segundo, o sistema de roteamento decide qual servidor no conjunto anycast receberá a consulta. Esse esquema é resultado de uma evolução que iniciou com 3 servidores raiz com endereços unicast, depois passou para 13 organizações de servidores raiz incluindo clusters com compartilhamento de carga e, em seguida, o esquema atual (com várias pequenas etapas no meio). Para simplificar, "13 servidores raiz" são na realidade "13 organizações de servidores raiz" que disponibilizam a zona para centenas ou milhares de servidores individuais[1]. O motivo pelo qual temos apenas 13 organizações de servidores raiz, e usamos anycast, é porque era muito mais fácil fazer isso do que liberar o limite de tamanho dos pacotes de UDP (User Datagram Protocol, Protocolo de Datagrama de Usuário) do DNS. Também há outros problemas de tamanho relacionados à adição de endereços IPv6. No caminho do servidor raiz para o usuário, a segurança poder ser opcionalmente fornecida pelo DNSSEC.

Ao longo dos anos, os servidores raiz sofreram ataques, principalmente do tipo DDOS (Distributed Denial Of Service, Negação de Serviço Distribuída). Para que um ataque como esse seja bem-sucedido contra um determinado usuário, as consultas a todos os endereços anycast das 13 diferentes organizações de servidor raiz deverão ser interrompidas. A interrupção de um subconjunto prejudicará o desempenho e o solicitante descobrirá quais servidores raiz deverá evitar. A interrupção poderá ser feita derrubando o servidor ou o caminho da rede para o servidor, geralmente por meio de uma sobrecarga. Então, por exemplo, em um ataque como esse, os usuários na Califórnia acharam que o servidor raiz em Estocolmo havia caído, e os usuários em Estocolmo, por sua vez, observaram exatamente o oposto. A resposta das organizações de servidor raiz a uma ameaça recente pela organização de hackers *anonymous* foi implementar mais largura de banda, servidores e FANFARE (Flow-Aware Network Framework for Attack Resistance through Enforcement, Estrutura de Rede com Reconhecimento de Fluxo para Resistência a Ataques por Execução).

Obviamente, o ataque não precisa ser direcionado contra a constelação de servidores raiz; ele pode ser direcionado contra a(s) conexão(ões) de usuários à Internet. Embora os danos sejam limitados, a correlação de forças entre um ataque de botnet e uma só empresa geralmente está muito mais a favor do invasor, até mesmo para grandes empresas.

Alguns painelistas têm recomendado às empresas que distribuam internamente cópias da raiz, **e quaisquer outras zonas críticas**, de modo que, durante um ataque, será possível continuar a operação normal, pelo menos para o DNS. A ICANN faz com que qualquer organização obtenha uma cópia da zona raiz de maneira simples e, com um pouco mais de trabalho, se torne uma instância de servidor raiz na organização de servidores raiz da ICANN. Também é uma boa ideia que as empresas sejam

[1] Atualmente, duas das organizações de servidor raiz são operadas pela mesma entidade, a Verisign.

autosuficientes internamente no que diz respeito ao DNS, e não sejam ameaçadas pela falta de acesso aos servidores externos nem pelas ações de um registro, registrador, operadores de servidor raiz etc., sejam elas acidentais ou intencionais.

Considerando o DNSSEC, temos um modo para distribuir uma zona que pode ser verificado usando assinaturas digitais integradas. Acreditamos que o princípio pode ser ampliado ainda mais, por exemplo, protegendo a delegação e dados *glue*. Também pode ser possível eliminar ou reduzir os dados de endereços e organização de servidor raiz. Um esquema, descrito em detalhes na contribuição de Paul Vixie, está incluído na seção Contribuições deste relatório.

Também há aspectos significativos referentes a políticas. Existem 13 organizações de servidores raiz, e vários países se sentem excluídos, mesmo considerando que eles podem instalar em seu país quantas instâncias de servidor raiz da ICANN quiserem. (Sem contar que muitas das outras organizações de servidores raiz estão dispostas a expandir suas constelações de anycast.) Então, vamos acabar com esse problema.

É importante notar que não há uma necessidade técnica de substituir o atual sistema de servidores raiz para aqueles que o preferem; vamos apenas simplificar a replicação para a raiz, e também dar um exemplo para outras zonas.

4.3.Controle compartilhado de zonas

Na seção anterior, discutimos as impressões políticas que fazem com que os países queiram ter uma organização de servidores raiz. Essas preocupações podem ou não ser bem fundamentadas, mas não há dúvida de que a atual operação raiz seja baseada nos EUA e está sujeita à jurisdição dos EUA.

Descrevendo de modo simples, a raiz é atualizada em uma sequência:

- A ICANN recebe solicitações de atualização dos TLDs e as examina em busca de erros
- A ICANN encaminha as alterações ao Departamento de Comércio (EUA)
- A ICANN envia as alterações aprovadas à Verisign
- A Verisign gera uma raiz assinada e a distribui

Existe algum modo técnico para pensar sobre o compartilhamento de controle da raiz? Algumas teorias foram elaboradas. Uma escola de pensamento é que os dados deveriam ter N múltiplas assinaturas. E, depois, M/N assinaturas seriam necessárias para autenticar os dados. Certamente, há argumentos quanto a M e N, e se seria necessária/desejada uma criptografia diferente.

Nossa intenção não é argumentar a favor de um sistema específico aqui, mas realmente achamos que um bom projeto permitiria dar início ao processo político para decidir como o controle deve ser compartilhado. Nossa visão é a criação de uma caixa de ferramentas para o controle compartilhado de zonas, não apenas para a raiz, mas também para outros problemas de coordenação de zonas. Observamos que o grupo de trabalho das Operações de DNS (DNSOPS) na IETF tem duas propostas para

coordenar as informações de assinatura do DNSSEC. No entanto, estamos nos questionando se não seria melhor criar uma facilidade geral em vez de uma solução para esse problema específico. A coordenação de endereços avançados e reversos pode ser outra aplicação.

Então, o que é necessário? Presumimos que o modelo certo seja um em que todas as partes que compartilham o controle tenham um conjunto de recursos:

- Um sistema para iniciar uma zona compartilhada consistindo na zona em si, regras e diários individuais para cada um dos participantes que publicar solicitações e ações
- Cada tipo de solicitação estará visível a todos os outros participantes que puderem aprovar, desaprovar ou indicar tempo limite esgotado
- As regras definem o que acontece a uma solicitação
    - Um tipo de regra é um voto que define as condições para que uma solicitação tenha êxito. Isso pode incluir um atraso para que todas as partes tenham tempo de considerar a solicitação.
        - Para ccTLDs, as regras da WSIS ditariam 1 de N, então, cada ccTLD (Country Code Top Level Domain, Domínio de Primeiro Nível com Código de País) poderia alterar seus próprios dados unilateralmente.
        - Outros domínios poderiam usar uma maioria simples
    - Atrasos especificados poderiam ser importantes para que os outros pudessem apontar problemas operacionais e permitir que os solicitantes reconsiderassem
    - Condições diferentes poderiam ser aplicadas para diferentes operações, como a criação de um novo vs. a edição etc.

Então, cada um dos participantes poderia fazer um algoritmo padrão para gerar estado consistente. Isso pode parecer uma fantasia, mas algoritmos bizantinos como o Bitcoin [Andreesen 2014] e o Namecoin mostram que esses sistemas são possíveis hoje em dia.

(Observação: não estamos propondo as regras, apenas um sistema distribuído para implementar as regras que a comunidade quiser, sejam elas quais forem.)

4.4.Operações de registro/registrador

Alguns painelistas argumentaram que as operações da ICANN deveriam fornecer garantias de nível de serviço, mas o painel não achou que poderia dar andamento a essa questão.

4.5.Quais dados devem ser publicados pela ICANN?

4.5.1. Parâmetros da ICANN

A ICANN gerencia muitos conjuntos de parâmetros como parte das funções da IANA (Internet Assigned Numbers Authority, Autoridade para Atribuição de Números na Internet), bem como do processo de

novos TLDs e de outros, por exemplo, rótulos reservados em vários idiomas. Todos esses devem ser disponibilizados on-line, talvez no DNS, e, certamente, de maneira segura, de modo que possam ser usados diretamente por qualquer um da comunidade da Internet.

4.5.2. Aniversários de domínios, atividades e bailiados

A reputação do DNS é uma ferramenta de segurança valiosa. A data de criação de um domínio é talvez a peça de informação mais significativa. Outra é a taxa de atualização de um domínio para endereços e nomes de servidores. Novos domínios e uma alta atividade de atualização são suspeitos. Seria interessante se essas informações estivessem disponíveis em tempo real.

As informações de bailiado foram discutidas de maneira semelhante, mas serão retomadas pela IETF no seu próximo encontro em março de 2014 em Londres.

4.5.3. O exemplo LISP

Anteriormente, o painel foi solicitado a considerar a possibilidade de a ICANN apoiar um serviço de super-raiz para o LISP (Locator/Identifier Separation Protocol, Protocolo de Separação de Identificadores/Localizadores) [RFC 6830]. Conforme nos foi explicado por Dino Farinacci e outros, a ICANN executaria servidores LISP como um serviço experimental para encaminhar solicitações para servidores LISP existentes que atualmente não oferecem conectividade universal. Localizamos recursos para quatro servidores, mas o projeto nunca foi iniciado devido a algumas questões não resolvidas:

- Qual seria o escopo (duração etc.) da experiência? Quais seriam os critérios para o sucesso?
- Que software seria usado e quem daria o suporte? Duas alternativas de propriedade particular foram disponibilizadas.
- Quem teria o controle operacional e de políticas?
- A ICANN deveria fazer isso ou os RIRs (Registros Regionais da Internet)?
- A resposta mudaria se os endereços IP não fossem envolvidos?

Os materiais sobre LISP estão em anexo como um apêndice. Nenhuma ação foi realizada quanto a essa experiência.

Alguns membros do painel acharam que “o LISP é apenas uma instância de uma classe mais genérica de tecnologias de tunelamento de transferência e, como tal, não apresenta nenhuma tarefa inovadora para o gerenciamento de identificadores que fugisse às atuais práticas operacionais para o gerenciamento de identificadores e, sendo assim, o argumento de que essa forma particular de tunelamento exigia uma atenção particular e o apoio da ICANN não foi claramente fundamentado”.

A ICANN deverá estar preparada para que perguntas técnicas e de políticas sobre novos identificadores sejam levantadas novamente, e fazer um planejamento adequado.

4.6. Colisões

Muitos painelistas estavam familiarizados com a questão de colisões no DNS e, apesar das extensas discussões sobre o assunto, nenhum novo direcionamento significativo foi dado. O painel achou, no entanto, que o protótipo real do sistema descrito em [ICANN 2013] é altamente recomendado.

5. Fundamentos do protocolo de DNS

Podemos imaginar uma revisão, upgrade ou renascimento na base do DNS? Muitos, inclusive alguns membros do painel, acreditam que a base instalada é muito resistente, ou que o processo está quebrado, ou que começar de novo é a melhor ideia.

Surpreendentemente, o painel foi unânime ao achar que valeria a pena um esforço para caracterizar os problemas e buscar soluções; nem que isso servisse apenas para encerrar o assunto. Nesta seção, descrevemos alguns problemas que deveriam ser estudados, caso fosse realizado um trabalho mais amplo.

A história das inovações no DNS tem seus momentos de sucessos e fracassos. Uma das principais lições aprendidas é que a tecnologia só é adotada amplamente se fornecer um benefício específico. Os administradores têm o cuidado de manter suas zonas conectadas ao DNS global e seus registros A e MX atualizados, caso contrário, eles não terão tráfego da Web e e-mail. No entanto, dos cerca de 60 tipos de registro que foram definidos, menos de 10 são usados amplamente.

Os esforços para criar aplicativos tiveram dificuldades semelhantes.

O primeiro conjunto de RFCs de DNS sugeriu um método para o roteamento de e-mail para caixas de correio específicas, mas ele nunca foi implementado. Um segundo esquema, o MX RR, resolveu o problema de fornecer servidores de e-mail redundante, bem como fornecer o roteamento de e-mail por meio de limites organizacionais (essa é a base do roteamento de e-mail hoje em dia). Bancos de dados antispam foram adotados amplamente sem padronização. Trabalhos concorrentes para padronizar a autenticação de e-mails resultou em duas implementações usando TXT RRs, e um debate sobre se a padronização de novos tipos seria algo útil.

O trabalho de mapeamento E.164 NUMber (ENUM) para padronizar o roteamento de telefones e outras mídias usando o DNS também obteve um sucesso muito limitado. Embora a tecnologia de NAPTR (Name Authority Pointer, Apontador de Autoridade de Nome) seja vista como uma verdadeira inovação, os projetistas de ENUM ignoraram a necessidade de fazer o roteamento com base em informações em vez do número de telefone de destino, e os fabricantes dos equipamentos preferiram manter o valor em seus sistemas de propriedade particular.

5.1.Princípios gerais

Qualquer novo projeto deverá:

- Remover os limites de tamanho — a MTU (Maximum Transmission Unit, Unidade Máxima de Transmissão) de 576 bytes provavelmente retardou o DNS mais do que qualquer outro fator; o DNSSEC não se adapta e, à exceção do Mecanismo de Extensão para DNS (EDNS0), muitos hardwares e softwares não passam pacotes grandes.
- Preservar a conectividade
- Tentar incentivar implementações consistentes. Se diferentes implementadores não seguirem as especificações, então, o usuário estará restrito à sobreposição comum existente, seja ela qual for.
- Permitir expansão futura
- Fornecer incentivos para a adoção

5.2.Modelo de dados

Os primeiros RFC de DNS imaginaram espaços de nomes paralelos para diferentes “classes” de informações, e novos tipos de dados desenvolvidos a partir de componentes simples. A noção de classe nunca foi explorada. Novos tipos de dados foram definidos, mas recentemente muitos argumentaram a favor do uso do registro TXT genérico destinado a cadeias de caracteres de texto arbitrário para carregar os dados, juntamente com outro nível de rótulo como substituto para o tipo RR.

Defendemos que o DNS deve definir seus próprios tipos e formatos de RR em metadados carregados no DNS, ou que nós formalizemos rótulos filho como o último tipo de dados e ampliemos o processo de consultas a fim de permitir uma correspondência mais flexível.

Por fim, precisamos explorar os objetos de dados autoassinados que podem existir independentes do nome de domínio.

5.3.Distribuição

A estrutura da zona de dados e cache pelo registro de recursos é implementada com alguns “aprimoramentos” desiguais ao padrão TTL (Time To Live, Tempo de Vida) e ao prefetch de informações prestes a expirar. Seria interessante considerar novas maneiras para agrupar dados com números de série que pudessem atualizar grupos de dados em cache sem realmente transferir os dados.

Também achamos que a segurança pode ser melhorada por meio da replicação mais frequente de zonas (possivelmente menores). Esses dados não precisam ser protegidos pelo DNSSEC. Sendo assim, é possível melhorar a segurança em lugares onde o DNSSEC não é implementado.

5.4.Application Program Interface (API)

A API (Application Program Interface, Interface de Programação de Aplicativos) do DNS apresenta duas formas: uma interface de usuário e nomes no nível da API. Em ambos os casos seria vantajoso termos uma sintaxe padrão que permitisse um FQDN (Fully Qualified Domain Name, Nome de Domínio

Totalmente Qualificado) explícito. A comunidade de usuários seria melhor atendida por um conjunto consistente de políticas de pesquisa em UIs (User Interfaces, Interfaces de Usuários), mas não está certa se conseguirá que os fornecedores façam isso.

A API de programação passou por várias tentativas de revisão, em sua maioria fracassada. Recentemente, assistimos a uma apresentação de Paul Hoffman sobre um novo projeto contendo interfaces assíncronas e suporte de DNSSEC. Consulte o apêndice. Sabemos que o trabalho está em andamento na Verisign Labs e na NLnet, mas não conseguimos obter mais informações, apesar de haver rumores de uma publicação iminente.

No entanto, independentemente da API, há uma questão relacionada que diz respeito ao local em que a validação do DNSSEC e a filtragem do DNS (se houver) devem ser realizadas. O painel foi unânime ao afirmar que o cancelamento de DNSSEC tecnicamente deverá ser permitido no sistema final (que pode ser uma máquina virtual, um laptop, um servidor no ambiente do usuário etc., dependendo da preferência do usuário), apesar de que isso poderá ser impossível por causa do roteador, do firewall ou de outras restrições herdadas. Da mesma maneira, embora a filtragem de DNS não seja a opção favorita de todos, ela estará sob controle do usuário.

Nada disso deverá impedir que o usuário terceirize essas tarefas para um ISP (Internet Service Provider, Provedor de Serviços de Internet) ou outro serviço.

Restrições legais ou de políticas poderão dizer o contrário.

Protocolo de consulta

5.5.Protocolo de consulta

O protocolo de consulta do DNS tem dois tipos de problemas: os que se referem à transferência de consultas/respostas de um solicitante para um servidor, e no que diz respeito a ampliar o poder da consulta.

Os problemas originais de transferência UDP começam pelo tradicional limite de MTU de 576 bytes. A correção original era recorrer ao TCP para transferências maiores. O tamanho dos dados da raiz foi talvez o primeiro elemento em que os limites de MTU tiveram um impacto muito amplo, resultando no limite de 13 servidores raiz; posteriormente, a adição de assinaturas de DNSSEC expandiram significativamente os pacotes de resposta. O EDNS0 foi concebido para solucionar esse problema, entre outros, obtendo algum sucesso. Contudo, há outros limites, como o tamanho do frame da Ethernet 1582, ou o 1280 do IPv6 etc., que fundamentalmente limitam o UDP.

Além disso, o EDNS0 não consegue solucionar o problema dos pontos de acesso, roteadores, firewalls e outros hardwares que bloqueiam o acesso à porta 53 TCP, ou limitam o tamanho de pacotes, ou até mesmo interceptam solicitações ao DNS em proxies transparentes, geralmente prejudicando o serviço. Problemas semelhantes podem ocorrer em servidores de nomes em cache que não incluem suporte para pacotes grandes, todos os tipos de dados de DNS, EDNS0 etc. Alguns problemas podem ser um tanto sutis. Em um exemplo, os pacotes de DNSSEC passam normalmente, mas não durante a renovação

de chaves do DNSSEC, um processo de manutenção normal, quando os pacotes se tornam um pouco maiores.

Um problema relacionado são os ataques de DDOS ao DNS, particularmente os que usam reflexão e amplificação. Nesses casos, é necessário ter alguma maneira de identificar o tráfego legítimo do tráfego do ataque. A validação do endereço de origem resolveria grande parte do problema, tanto para o DNS quanto para muitos outros protocolos. O painel apoia esse processo, mas ele não é implementado amplamente. Rate shaping (modelagem de taxa) e várias heurísticas podem ajudar, mas não são uma solução definitiva. Diversos mecanismos leves de autenticação foram e permanecem sendo candidatos.

Uma escola de pensamento sobre a solução para o problema de transferência é colocar todo o tráfego do DNS em https:. A lógica é que todos têm o interesse inerente de ver o fluxo seguro do tráfego na Web e, sendo assim, torna-se um caminho garantido (alguns afirmam que é o ÚNICO caminho garantido). O preço a ser pago é o estado da conexão e a sobrecarga relacionada. As alternativas envolvem algum novo protocolo de transação ou um modo de usar o UDP, sendo que ambas poderão não funcionar em partes da base instalada. De qualquer forma, há a questão de as transações de DNS usarem um formato tradicional ou novo.

Independentemente da transferência, o protocolo de consulta do DNS deve ser expandido para permitir consultas mais flexíveis. Elas podem incluir algum tipo de controle de acesso para rótulos sucessores substituindo o NSEC.

Os protocolos de pesquisa mundial, como o CCN, aprenderam com o DNS e incorporaram todos esses recursos. O problema está mais relacionado a descobrir como motivar um upgrade da infraestrutura existente com alguma compatibilidade reversa, em vez de uma inovação na ciência de protocolos.

6. Observações e recomendações

- O uso do DNS na infraestrutura continuará crescendo; o uso do DNS na UI (User Interface, Interface do Usuário) é prejudicado pelas alternativas baseadas em pesquisa, interfaces móveis etc.
- A ICANN deverá publicar mais dados assinados de DNSSEC para rótulos reservados etc.
- Em cooperação com a IETF e outros, realizar um estudo para definir uma visão da arquitetura do DNS para 2020.
- Projetar e fazer o protótipo da publicação de raiz aberta.
- Projetar um sistema de controle compartilhado de zonas para a raiz.
- Realizar exercícios de colisão para testar a facilidade de implementação [ICANN 2013].

7. Referências

[Andreesen 2014] Andreesen, “Why Bitcoin Matters”, http://dealbook.nytimes.com/2014/01/21/why-bitcoin-matters

[DNS/TCP] https://lists.dns-oarc.net/mailman/listinfo/tcp-testing

[Fayazbakhsh 2013] Fayazbakhsh et al, “Less Pain, Most of the Gain: Incrementally Deployable ICN”, Sigcomm 2013

[Ghodsi 2011] Ghodsi et al, “Naming in Content-Oriented Architecture”, Sigcomm 2011

[Huston 2013] Estudo sobre DNS por TCP somente http://www.circleid.com/posts/20130820_a_question_of_dns_protocols/ e o que está por vir nas operações de DNS.

[ICANN 2013] “Guia para a Identificação e Mitigação de Colisão de Nomes para Profissionais de TI”, https://www.icann.org/pt/about/staff/security/ssr/name-collision-mitigation-05dec13-pt.pdf

[Kaminsky 2004] D. Kaminsky, “Tunneling Audio, Video, and SSH over DNS”, BlackHat 2004

[Merit] Seções sobre domínios e DNS http://www.afnic.fr/en/about-afnic/news/general-news/6391/show/the-internet-in-10-years-professionals-answer-the-afnic-survey.html

[Mockapetris 88] P. Mockapetris e K. Dunlap, “Development of the Domain Name System”, SIGCOMM 88

[Newyorker 2013] http://www.newyorker.com/online/blogs/elements/2013/12/the-mission-to-decentralize-the-internet.html?goback=%2Egde_1430_member_5817512945197801473#%21

[RFC 881] J. Postel, “The Domain Names Plan and Schedule”, novembro de 1983

[RFC 882] P. Mockapetris, “Domain Names – Concepts and Facilities”, novembro de 1983

[RFC 883] P. Mockapetris, “Domain Names – Implementation and Specification”, novembro de 1983

[RFC 1034] P. Mockapetris, “Domain Names – Concepts and Facilities”, novembro de 1987

[RFC 1035] P. Mockapetris, “Domain Names – Implementation and Specification”, novembro de 1987

[Spiegel 2014] http://www.spiegel.de/international/world/nsa-secret-toolbox-ant-unit-offers-spy-gadgets-for-every-need-a-941006.html

8. Glossário

AI	Artificial Intelligence (Inteligência Artificial)
API	Application Program Interface (Interface de Programação de Aplicativos)
CCN	Content Centric Networking (Sistema de Redes Centrado em Conteúdo)
ccTLD	Country Code Top Level Domain (Domínio de Primeiro Nível com Código de País) — um TLD atribuído a um determinado país
DANE	DNS-based Authentication of Named Entities (Autenticação Baseada em DNS de Entidades Nomeadas)
DDOS	Distributed Denial Of Service (Negação de Serviço Distribuída)
DNS	Domain Name System (Sistema de Nomes de Domínio) — o sistema de nomenclatura da Internet
DNSOPS	Operações de DNS — um grupo de trabalho da IETF dedicados aos problemas das Operações do DNS, entre outros.
DNSSEC	Domain Name System Security Extensions (Extensões de Segurança do Sistema de Nomes de Domínio)
DSL	Digital Subscriber Line (Linha de Assinante Digital)
E.164	uma recomendação UIT-T, intitulada *The international public telecommunication numbering plan* (O plano internacional de numeração de telecomunicações públicas), que define um plano de numeração para a rede pública de telefonia comutada (RPTC) mundial e algumas outras redes de dados
EDNS0	Mecanismo de Extensão para o DNS [RFC 2671] — Um padrão para ampliar o tamanho e os campos das especificações originais do DNS
ENUM	Mapeamento E.164 NUMber — um sistema para unificar o sistema internacional de numeração de telefones da rede pública de telefonia comutada com o endereçamento da Internet e os espaços de nomes de identificação para, por exemplo, fazer o roteamento de uma chamada telefônica
FEDEX	Federal Express
FQDN	Fully Qualified Domain Name (Nome de Domínio Totalmente Qualificado)
FTP	File Transfer Protocol (Protocolo de Transferência de Arquivos)

gTLD	Generic Top Level Domain (Domínio Genérico de Primeiro Nível) — um TLD que não corresponde a um código de país
HTTPS	Hypertext Transfer Protocol Secure (Protocolo de Transferência de Hipertexto Seguro)
IANA	Internet Assigned Numbers Authority (Autoridade para Atribuição de Números na Internet)
ICANN	Internet Corporation for Assigned Names and Numbers (Corporação da Internet para Atribuição de Nomes e Números)
ICN	Information Centric Networking (Sistema de Redes Centrado em Informações)
IEEE	Institute of Electrical and Electronics Engineers (Instituto de Engenheiros Eletricistas e Eletrônicos)
IETF	Internet Engineering Task Force (Força-tarefa de Engenharia da Internet)
IP	Internet Protocol (Protocolo de Internet)
IPSEC	Internet Protocol Security (Segurança de Protocolo de Internet)
IPv4	Internet Protocol version 4 (Protocolo de Internet versão 4)
IPv6	Internet Protocol version 6 (Protocolo de Internet versão 6)
ITI	Identifier Technology Innovation (Inovação da Tecnologia de Identificadores) — um painel estratégico da ICANN
LISP	Locator/Identifier Separation Protocol (Protocolo de Separação de Identificadores/Localizadores) [RFC 6830]
MIB	Management Information Base (Base de Informações de Gerenciamento)
MTU	Maximum Transmission Unit (Unidade Máxima de Transmissão) — o tamanho da unidade máxima de dados que pode passar ou passar sem fragmentação
MX	Mail eXchange — um tipo de dados de DNS que especifica a troca de e-mails que administra os e-mails de um domínio específico
NAPTR	Name Authority PoinTeR (Apontador de Autoridade de Nome) — um tipo de dados de DNS usado com mais frequência na telefonia pela Internet
NDN	Named Data Networking (Sistema de Redes de Dados Nomeados)
P2P	Peer to Peer
PKI	Public Key Infrastructure (Infraestrutura de Chaves Públicas)

RFC Request For Comments (Solicitação de Comentários) — memorandos que documentam os problemas técnicos e operacionais da Internet

RIR Regional Internet Registry (Registros Regionais da Internet) — uma das organizações que gerenciam a alocação e o registro de recursos numéricos da Internet em uma determinada região do mundo. Por exemplo, a ARIN (American Registry for Internet Numbers, Registro Americano para Números da Internet) é responsável pelo Canadá, os Estados Unidos e muitas ilhas do Caribe e do Atlântico Norte.

Rsynch Protocolo de sincronização remota — sincroniza arquivos e diretórias ao mesmo tempo que minimiza a transferência de dados usando codificação delta

RR Resource Record (Registro de Recurso) — a unidade atômica de informação no DNS

TSIG Transaction Signature (Assinatura de Transação)

TTL Time To Live (Tempo de Vida)

TXT O tipo de RR de texto no DNS que permite campos de texto de formato livre

UDP User Datagram Protocol (Protocolo de Datagrama de Usuário) — o protocolo de datagrama sem conexão da Internet

UI User Interface (Interface do Usuário)

URI Uniform Resource Identifier (Identificador Uniforme de Recursos)

URL Uniform Resource Locator (Localizador Uniforme de Recursos)

Wi-Fi Wireless Fidelity (Fidelidade Sem Fio) — as normas para redes sem fio definidas pela família de normas IEEE 802.11

9. Contribuições de membros do painel

Todas as contribuições foram reproduzidas fielmente, conforme enviadas pelo autor.

9.1.Contribuição de James Seng

Arquitetura técnica

O hacker que mora dentro de mim gosta da arquitetura descentralizada. É possível afirmar que muitos dos “problemas políticos” que temos hoje derivam da natureza centralizada do DNS com a raiz.

Então, tecnologias como namecoins ou outro sistema de identificadores decentralizado me deixam confuso.

No entanto, não há um sistema de identificadores decentralizado mas coordenado que eu conheça que tem sido realmente usado amplamente. Assim, gostem ou não, o sistema DNS ainda é um dos sistemas de identificadores implementado que temos. Como fazemos na IETF, sãos os “códigos em execução” que vencem, e não necessariamente os que têm o melhor projeto.

Não acredito em uma multiraiz ou em uma raiz alternativa. Como disse em Buenos Aires, defendo a RFC 2826. Multiraiz, raiz alternativa e todas as propostas relacionadas só movem o problema político para outra camada, mas não resolvem o problema político fundamental. Observem que disse problema político, porque não acho que a multiraiz resolveria nenhum problema técnico sequer; a única coisa que faria seria aumentar a complexidade técnica.

ICANN

O DNS e sua natureza centralizada da raiz foi responsável, em parte, por transformar a operação original simples de função da IANA na enorme organização que hoje chamamos de ICANN.

Tenho participado na ICANN desde seu primeiro encontro, em 1999, e compareci a quase todos eles. Ao longo desses anos, existem coisas que eu gostaria que a ICANN tivesse feito de maneira diferente, ou seja, nossa posição não está sempre alinhada.

No entanto, a ICANN é o “código em execução” da coordenação dos identificadores do DNS. Talvez existam outros projetos melhores, quem sabe mais simples e elegantes (pois muitos membros da comunidade da IETF gostariam poder voltar aos dias de Jon Postel), mas as coisas são o que são hoje e, o que é mais importante, embora pudessem ser melhores, elas funcionam. A alternativa proposta (UIT) que conhecemos tem outros problemas ou ainda piores.Â

Por isso, apoio a ICANN, porque é simplesmente o melhor sistema em funcionamento que temos para a coordenação dos identificadores do DNS e da raiz.

A ampliação do DNS e de seu sistema para outras áreas

Sendo assim, tenho pouco interesse em reprojetar o DNS ou alternativas propostas para identificadores de nomes. Com o tempo, alguém, alguma organização deverá existir para fazer a coordenação e enfrentaremos os mesmos problemas políticos novamente.

Eu apoio e gostaria de ver o ecossistema do DNS (normas de DNS, operação da raiz, ICANN...) que temos, originalmente projetado para o DNS e que evoluiu, ser ampliado para outras áreas (por exemplo, RFID), para que mais comunidades possam ser incluídas. O trabalho que fizemos nos IDNs (Internationalized Domain Names, Nomes de Domínios Internacionalizados), de certa forma, está incluindo um grupo de comunidades de usuários que precisa usar seus próprios idiomas nativos no ecossistema de DNS; em vez de deixá-los desenvolver o seu próprio.

Embora alguns tenham argumentado comigo que se tivéssemos feito os IDNs fora do ecossistema de DNS a implementação teria sido muito mais rápida (por exemplo, consulte palavras-chave em idiomas nativos), eu digo que os IDNs também são melhores porque fazem parte do ecossistema de DNS, que tem padrões abertos bem definidos, implementações abertas, empresas que se desenvolvem com base na legitimidade do DNS e, da mesma maneira, a proteção dos usuários finais e registrantes de IDNs.

Sendo assim, não tenho remorsos e apoio explorarmos a ideia de como poderemos ampliar o DNS para identificadores, para os quais não foi intencionado e projetado originalmente. Os engenheiros que desenvolvem identificadores geralmente são ingênuos quanto às políticas que acompanham esses identificadores, especialmente se esses identificadores são expostos a usuários finais. Eles podem aprender uma coisa ou duas com a história dos identificadores de DNS e a ICANN.Â

Políticas da raiz

As políticas da ICANN e os pontos de vista da ICANN enquanto parte da “Governança da Internet” são derivados da função da ICANN de coordenar os servidores raiz.

Para piorar, 11 dos 13 servidores raiz são baseados nos EUA, devido a um acidente histórico, mas, mesmo assim, piora ainda mais a percepção de que a ICANN está sob controle dos EUA, especialmente nos dias atuais pós-Snowden.

Sempre que alguém aparece para falar que certo país deveria ter um servidor raiz, nós afastamos a ideia usando motivos históricos ou técnicos de que não há como ampliar para mais de 13 raízes.

A história eu posso aceitar como um motivo.

Os motivos técnicos eu não posso. Isso é uma desculpa, porque não estou ciente de nenhum trabalho da IETF dedicado a realmente tentar ampliar para mais de 13 raízes. É por isso que disse no encontro de Buenos Aires que posso pensar em algumas soluções técnicas, que pelo menos sejam suficientes como um I-D. Não podemos deixar a ICANN continuar usando motivos da IETF/técnicos como uma desculpa para os problemas políticos que estão enfrentando. Devemos ser capazes de dizer à ICANN que “sim, pode ser feito, mas não cabe a você decidir as políticas para fazer isso ou não”.

Além disso, o que é ainda mais importante, a operação dos servidores raiz não é algo tão exagerado.

Ter uma raiz não significa que o responsável terá controle imediato sobre a Internet. Na verdade, isso é tão tedioso quanto uma Raiz Anycast. Apesar de que, se o operador da raiz não seguir as Práticas Recomendadas para a Operação do Servidor Raiz (por exemplo, a RFC 2010 e a RFC 2870), isso pode causar muito dano à Internet.

A maioria dos engenheiros deve ter entendido o que eu disse acima, mas a maioria dos membros da ICANN não.

Então, há considerações a serem feitas ao selecionar um operador de servidor raiz, porque ele é essencial para a estabilidade dos identificadores da Internet, e grande parte disso se baseia na Confiança. Entretanto, Confiança, gostem ou não, não é um problema de engenharia.

James Seng

http://chineseseoshifu.com/blog/dnspod-in-china.html

Porque o DNSPod é importante na China, apesar do modo como “quebrou” o DNS.

9.2. Resolução de DNS e comportamento de aplicativo de lista de busca — Geoff Huston

nenhum – NÃO realiza nenhuma busca no DNS

nunca – pesquisa o nome da base, mas não aplica a lista de busca

pré – aplica a lista de busca e, se isso retornar NXDOMAIN, então, pesquisa o nome da base

pós – pesquisa o nome da base e, se isso retornar NXDOMAIN, então, aplica a lista de busca

sempre – NÃO pesquisa o nome da base; só aplica a list de busca

Comportamento da biblioteca de resolvedores de DNS no sistema operacional base

Sistema	**Absoluto** *servidor.*	**Rótulo único relativo** *servidor*	**Multirrótulo relativo** *www.servidor*
MAC OSX 10.9	nunca	sempre	nunca
Windows XP	nunca	sempre	pós
Windows Vista	nunca	sempre	nunca
Windows 7	nunca	sempre	nunca
Windows 8	nunca	sempre	nunca
FreeBSD 9.1	nunca	pré	pós
Ubuntu 13.04	nunca	pré	pós

Comportamento de navegadores em plataformas MAC e Windows

MAC OSX 10.9

	servidor.	*servidor*	*www.servidor*
Chrome (31.0.1650.39 beta)	nunca	sempre	pré
Opera (12.16)	nunca	sempre	nunca
Firefox (25.0)	pós*	sempre	pós*
Safari (7.0 9537.71)	nenhum**	nenhum**	nenhum**

* Adicionou o prefixo “www.”, depois tentou prefixar “www.” e também anexar a lista de busca

** O Safari parece reconhecer TLDs e não realiza buscas no DNS quando o nome não for um TLD

Windows 8.1

	servidor.	*servidor*	*www.servidor*
Explorer (11.0.900.16384)	nenhum	nenhum	nunca
Firefox (25.0)	nunca*	sempre	nunca
Opera (17.0)	nenhum	nenhum	nenhum**
Safari (5.1.7 7534.57.2)	nunca*	sempre***	nunca

* Adicionou o prefixo “www”

** O OPERA reconhece TLDs delegado e só pergunta quando o último rótulo for um TLD

*** Adicionou o prefixo “www” e o sufixo “.com”

9.3. Observações sobre consistência e contribuição de tendência — Geoff Huston

Se olharmos a origem do Sistema de Nomes de Domínio, encontraremos os chamados “hosts file” (arquivo hosts), uma tentativa de trazer os nomes de uso humano para o contexto das redes de computadores. A ARPANET usou um modelo de nomenclatura de nó de rede em que cada nó conectado tinha um arquivo de configuração local, o arquivo hosts, que continha os nomes de todos os outros nós da ARPANET, e os endereços de protocolo de cada nó. Não havia nenhuma consistência aplicada nessas múltiplas instâncias desse arquivo hosts em todo o conjunto de nós conectados à ARPANET, nem, naquele momento, havia nenhum método para distribuir uma cópia do arquivo hosts pela rede. A utilidade desse arquivo hosts era fornecer nomes mais fáceis para as pessoas no lugar dos endereços mais obtusos a nível de protocolo. Os usuários eram capazes de identificar os nós das redes pelo seu nome simbólico, que era então traduzido para um endereço binário específico do protocolo por meio de uma pesquisa no arquivo hosts. À medida que a ARPANET cresceu, também foi observado um aumento do tamanho e da taxa de atualização do arquivo hosts, bem como a sobrecarga de manter um arquivo hosts local preciso. O formato de arquivo hosts foi padronizado (RFC 952) e um serviço de arquivo hosts central foi definido (RFC 953) que poderia tomar o lugar de muitas cópias locais do arquivo hosts.

Mais tarde, esse formato foi substituído pelo DNS (Domain Name System, Sistema de Nomes de Domínio), originalmente especificado em 1983, na RFC 882 e na RFC 883. O mecanismo de tradução de um nome (especificado como uma cadeia de caracteres fácil para as pessoas) para um endereço de serviço de protocolo específico foi mantido pela transição do arquivo hosts para o DNS.

Esse espaço de identificador tem várias propriedades, incluindo a observação de que o DNS atravessa um espaço de nomes que é adequado para uso no discurso humano, ao mesmo tempo que admite uma estrutura formal suficiente para permitir que nomes sejam manipulados por aplicativos de computadores de maneira determinística. O espaço de nomes do DNS é um espaço de estrutura hierárquica, permitindo que o espaço de nomes seja pesquisado com eficiência por correspondências exatas, e, ao mesmo tempo, permitindo uma estrutura de gerenciamento distribuído do espaço de nomes. Contanto que as colisões de rótulos sejam evitadas em qualquer zona individual da hierarquia de nomes do DNS, as colisões de nomes poderão ser evitadas no espaço de nomes geral do DNS, permitindo que a exclusividade de nomes seja prontamente gerenciada no contexto do DNS. O DNS é flexível no que diz respeito à sua função de mapeamento, e pode ser usado para associar um espaço de nomes estruturado para qualquer outra forma do recurso nomeado ou ponto de serviço. O DNS foi desenvolvido para ser consistente. Sendo assim, considerando uma entrada de nome consistente no DNS, as consultas para esse nome devem fornecer a mesma resposta nos diversos locais do consultante e nos diversos horários da consulta. Isso permite uma consistência referencial, em que um nome no DNS pode ser passado entre partes diferentes e fazer referência a um recurso consistente de local de serviço. O DNS não tem como objetivo substituir um sistema de diretórios ou um sistema de busca. Se houver uma correspondência exata do nome sendo consultado no DNS, a consulta no DNS retornará o valor mapeado como resultado da consulta; caso contrário, a consulta retornará um erro de correspondência.

Desde então, esse modelo do espaço de nomes do DNS como o espaço de nomes de identificadores usado para dar suporte a uma interface humana com a rede passou por várias alterações, principalmente em resposta ao modo de uso humano de identificadores no discurso. Temos a tendência de usar identificadores de maneira menos precisa e de modo a incluir elementos de contexto local, que usam idiomas e escritas locais. Com o tempo, a função do DNS enquanto uma forma de interface humana para os recursos e os serviços da rede foi abrangida por esforços para dar suporte a interfaces que funcionassem de maneira mais “natural” para o uso humano.

A RFC 1034 propôs o uso de uma forma de estenografia na especificação de nomes do DNS, onde os nomes que não terminassem com ‘.’ à direita eram chamados de “nomes relativos”, e, conforme observado na RFC 1034, “nomes relativos aparecem principalmente na interface do usuário, onde sua interpretação varia de uma implementação para outra”. Geralmente, essa interpretação local envolvia a conciliação de uma lista de busca local de sufixos de rótulos, permitindo que o usuário especificasse a parte inicial de um nome de domínio e confiasse no aplicativo local ou nas rotinas do software de resolução de nomes para adicionar um sufixo definido localmente para formar um nome de DNS completo.

Essa forma de oclusão seletiva do espaço de identificadores do DNS pelo uso de sufixos de nomes foi levada um passo à frente na interface do usuário fornecida pelos navegadores da Web, onde a prática comum nos navegadores da Web era pegar o componente identificador do DNS de um URL e aplicar uma transformação de nome prefixando a cadeia de caracteres “www.” e adicionando um sufixo definido localmente (geralmente “.com”). Dessa maneira, o identificador que o usuário especificou e o nome de identificador usado na consulta subsequente no DNS estavam relacionados, mas não eram necessariamente iguais.

Esse uso de transformações de nomes locais foi estendida ainda mais na maneira pela qual os identificadores formados por escritas de idiomas (diferentes dos códigos ASCII dos EUA) eram mapeados no DNS (IDNs: RFC 5891). Tratava-se de um processo definido explicitamente em que o identificador informado pelo usuário era transformado em uma cadeia de caracteres de rótulo codificada que formava a consulta no DNS. Nesse caso, a transformação era definida precisamente, de modo que múltiplas implementações do padrão de IDN têm como objetivo dar suporte a uma exibição consistente do mapeamento de um identificador em uma determinada escrita para uma forma de nome de DNS codificado.

Um evolução ainda maior do aperfeiçoamento do modelo de interação humana foi a unificação de termos de busca e URLs enquanto entradas em navegadores. Nesse caso, se o usuário não usar a especificação completa de um URL no navegador, o navegador tentará fazer a correspondência.

9.4.Contribuição de Paul Vixie

Anycast universal para a zona raiz

Visão geral

Propomos que a IANA produza diversas formas adicionais da zona raiz do DNS, a fim de permitir o anycast universal e a pesquisa operacional. “Anycast universal” nesse contexto significa uma zona raiz cujos registros de NS no ápice listam somente dois servidores de nomes, cujos endereços “bem conhecidos” associados (conforme fornecidos pelos registros A e AAAA) possam ser hospedados por qualquer um. “Pesquisa operacional” nesse contexto inclui o teste público em grande escala de serviço de nome raiz somente com IPv6 e o teste público em grande escala dos efeitos da colisão de “novos gTLDs”. Essa abordagem trata o serviço de nome raiz como uma utilidade não gerenciada, em vez de uma utilidade gerenciada.

Histórico

O anycast universal para a zona raiz não pôde ser implementado com segurança e responsabilidade antes do advento do DNSSEC, já que sem o DNSSEC, qualquer servidor respondente poderia ser configurado com dados de raiz do DNS arbitrários, incluindo novos TLDs ou TLDs existentes redelegados. Com o DNSSEC, agora é possível para os operadores de servidores de nomes recursivos configurar a validação de DNSSEC, de modo que qualquer informação de gTLD recebida de um servidor de nome de raiz anycast universal deve ser aprovado pela IANA, conforme indicado pelas assinaturas de DNSSEC geradas com a ZSK (Zone Signing Key, Chave de Assinatura de Zona) de raiz da IANA.

As críticas ao atual e histórico Sistema de Servidor de Nomes Raiz incluem a fraca resistência a ataques de DDoS, observando que, mesmo com o atual processo de anycasting em grande escala realizado por todos os Operadores de Servidor de Nomes Raiz, ainda há apenas algumas centenas de servidores de nomes no mundo que podem responder com autoridade pela zona raiz do DNS. Também estamos preocupados com o fato de que a capacidade de alcance do Sistema de Servidor de Nomes Raiz seja exigida até mesmo para a comunicação puramente local, uma vez que, do contrário, os clientes locais não dispõem de outra maneira para encontrar serviços locais. Em um sistema distribuído de proporções mundiais como a Internet, os serviços essenciais devem ser extremamente bem distribuídos.

Detalhes

Existem diversas variações úteis que podem ser formuladas. Primeiro, o anycast universal básico permitirá que qualquer operador de servidor de nomes capture o tráfego direcionado ao sistema de servidor de nomes raiz e responda localmente. A IANA geraria e assinaria digitalmente (com o DNSSEC) uma versão adicional da zona raiz que tivesse um conjunto diferente de registros NS no seu ápice. Esses registros de NS denotarão os servidores de nomes cujos endereços não estejam atribuídos a nenhum RNSO (Root Name Server Operator, Operador de Servidor de Nomes Raiz) em particular, mas que, em vez disso, são mantidos em confiança pela IANA para serem usados por qualquer parte interessada ou todas elas. A IANA solicitaria microalocações de infraestrutura para um RIR (como o ARIN ou o APNIC),

bem como vários prefixos IPv4 de 24 bits e vários prefixos IPv6 de 48 bits, para serem usados no processo de anycast universal da zona raiz.

Uma segunda variação para a atual zona raiz seria fornecer anycast universal conforme mencionado acima, mas que denotasse servidores de nomes que tivessem apenas conectividade IPv6 (indicada pela presença de registros AAAA) e nenhuma conectividade IPv4 (conforme indicada pela ausência de registros A). Essa variação facilitaria a pesquisa operacional no sistema de redes com somente IPv6.

Uma terceira variação para a atual zona raiz forneceria anycast universal conforme mencionado anteriormente, mas incluiria delegações para todos os novos gTLDs conhecidos, incluindo aqueles que não estão prontos para delegação (como .CORP e .HOME). Esses novos gTLDs seriam delegados para um servidor de nomes operado pela própria IANA, para fins de medição. A cada novo gTLD serão atribuídos registros A e AAAA curinga, cujos endereços chegarão a servidores da Web operados pela IANA para fins de medição.

Impacto

Considerando a natureza hierárquica do roteamento da Internet, os blocos de endereços anycast poderão ser comunicados em múltiplos níveis. Uma VM (Virtual Machine, Máquina Virtual) sendo executada em um laptop poderá ter seu próprio processo de servidor de nomes que escute os endereços bem conhecidos apropriados, sendo que, nesse caso, nenhuma consulta de serviço de nome raiz sairá dessa VM. O laptop em si poderia também capturar tráfego fora dos limites direcionado para esses endereços bem conhecidos, que atenderiam outras VMs ou outros processos sendo executados nesse laptop. O upstream do roteador sem fio desse laptop poderia ter servidores escutando esses endereços, sendo que, nesse caso, nenhuma consulta de servidor de nome raiz sairia dessa LAN sem fio. O ISP poderia operar servidores que escutassem esses endereços bem conhecidos, para atender a todo e qualquer consumidor que não operar seu próprio servidor. Por fim, espera-se que a Internet global tenha muitos operadores que comuniquem rotas para esses blocos de endereços bem conhecidos, incluindo, pelo menos, os doze operadores existentes do servidor de nomes raiz.

O impacto positivo disso seria maior possível resiliência e a redução da latência do serviço de nomes raiz. O impacto negativo disso seria redução da capacidade de diagnóstico e a maior vulnerabilidade a “envenenamento de rota” ou “sequestro” do tráfego do serviço de nomes raiz. De qualquer forma, é essencial que a validação do DNSSEC se torne comum a fim de reduzir as consequências para esse tipo de sequestro. Queremos que o resultado para um invasor seja “vítima perde o serviço de nomes raiz”, em vez de “vítima vê um espaço de nomes de DNS diferente”.

Exemplos

Os exemplos a seguir mostram o conjunto de registros de NS no ápice para cada variante de zona raiz, incluindo o endereço glue. Esses dados seriam incluídos em uma variante da zona raiz antes da assinatura do DNSSEC, e também seriam publicados como um arquivo “root hints” (dicas da raiz). Os dados exibidos para iana-servers.net (servidores da IANA) também estariam presentes no zona real de iana-servers.net. Estes exemplos exigiram quatro microalocações IPv4 e seis microalocações IPv6.

Variante 1: anycast universal

. IN NS anycast-1.iana-servers.net.

. IN NS anycast-2.iana-servers.net.

$ORIGIN iana-servers.net.

anycast-1 IN AAAA 2001:?:1::1

anycast-1 IN A ?.?.1.1

anycast-2 IN AAAA 2001:?:2::2

anycast-2 IN A ?.?.2.2

Variante 2: anycast universal somente IPv6

. IN NS v6only-1.iana-servers.net.

. IN NS v6only-2.iana-servers.net.

$ORIGIN iana-servers.net.

v6only-1 IN AAAA 2001:?:3::1

v6only-2 IN AAAA 2001:?:4::2

Variante 3: anycast para estudo de colisão de gTLDs

. IN NS gtldstudy-1.iana-servers.net.

. IN NS gtldstudy-2.iana-servers.net.

$ORIGIN iana-servers.net.

gtldstudy-1 IN AAAA 2001:?:5::1

gtldstudy-1 IN A ?.?.5.1

gtldstudy-2 IN AAAA 2001:?:6::2

gtldstudy-2 IN A ?.?.6.2

10. Apêndices

10.1. Materiais sobre LISP