Relatório de viagem ao Nanog 73
Denver - Colorado
Henrique Faulhaber
25-27 Junho/2018

Prezados conselheiros,

Participei do evento Nanog 73 em Denver nos Estados Unidos entre 26 e 27 de Junho de 2018. Também estavam lá funcionários do NIC.br da diretoria de Projetos, que trabalham no projeto IX.br

O Nanog (North American Network Operators Group) reúne os operadores de rede da América do Norte (Estados Unidos e Canadá) e visa a discussão das boas práticas de operação de redes e de sua interconexão. É um evento muito importante pois lá são discutidos os principais temas referentes a operação de redes e é uma oportunidade de intercambio com os principais operadores de rede e fornecedores de soluções para aquela região.

As reuniões do NANOG são quadrimestrais, e acontecem em diferentes regiões dos Estados Unidos e Canada 3 vezes ao ano. A edição 73 do Nanog contou com mais de mil participantes, e se estendeu por 3 dias com seminários, mesas redondas e exibição de fornecedores.

Para mim os destaques desse Nanog foram algumas conferências e o "peering coordinating fórum" que resumo abaixo:

Palestra do diretor de Operações do Facebook

Najam Ahmad, diretor do Facebook falou sobre a a abordagem gerencial da plataforma sobre a prevenção e tratamento de falhas, enfatizando a necessidade de haver uma mentalidade de operações e uma rigorosa ação preventiva e corretiva para falhas.

Ele disse que não se trata simplesmente de "automatizar" coisas ou de ter uma equipe de desenvolvedores a mão. Nesta palestra foram mostrados os esforços de recuperação de desastres do Facebook, como um estudo de caso para descrever essa filosofia operacional e mostrar abordagens para implantar infraestrutura que sobreviva a desastres sem intervenção humana significativa.

Palestra da T Mobile sobre adoção de IPV6
Palestrante: Stephan Lagerholm

A T-Mobile em 10 anos teve uma estratégia de remover sua dependência do IPv4. EM 2017 foi desativado o IPv4 para mais de 10 milhões de aparelhos. Em março de 2018, menos de 10% de seus usuários dependem de IPV4. Para conseguir isso, a T-mobile usou a tradução de endereços IPV4 em IPV6 (NAT64) , método DNS64 e tecnologias 464XLAT para contornar o problema de aplicativos que não eram capazes de trabalhar em IPv6 e que necessitam de um endereço IPV4 privado.

O palestrante destacou a importância do Android a partir da versão 4.3 dar suporte a IPV6 e ao fato do IOS9 oferecer serviços somente para IPV6.
Os terminais ainda operando em IPV4 na rede da T-mobile são os mais antigos, os que estão em roaming em outras operadoras, e alguns clientes corporativos que usam dual stack.

Stephan Lagerholn atribui o sucesso da migração da T-mobile ao investimento de 10 anos em IPV6, ao atendimento aos clientes nas redes sociais, e as ações proativas visando determinar que sites e aplicativos seriam os mais relevantes para essa migração.

Palestra sobre MANRS

Outra palestra muito interessante foi a de Andrei Robachevsky, que é o gerente sênior do programa técnico da Interenet Society e que falou sobre a segurança no roteamento e sobre o Programa MANRS em que o NIC.br participa desde o final do ano passado.

A iniciativa MANRS (Mutually Agreed Norms for Routing Security) é um projeto global de operadores de redes e IXPs para reduzir as principais ameaças de segurança aos protocolos de roteamento.

Um só operador não pode proteger sua própria rede sozinho. Mas é possível ajudar o sistema global de roteamento como um todo participando em ações conjuntas. O MANRS oferece uma oportunidade para uma abordagem sistêmica reconhecida globalmente para o roteamento com segurança.

O principio norteador do MANRS é que os operadores de rede têm a responsabilidade de garantir uma infraestrutura de roteamento robusta e segura. A segurança da sua rede depende de uma infraestrutura de roteamento que elimine os agentes mal-intencionados e configurações incorretas acidentais que causam estragos na Internet. Quanto mais operadoras de rede trabalharem juntas, menos incidentes haverá e menos danos poderão causar

O sistema de roteamento está constantemente sendo atacado. Em 2017 tivemos cerca de 14 mil incidentes, e mais de 10% dos sistemas autônomos da internet forma afetados (3100 + ASs). Sendo que os países mais afetados foram Brasil e Estados Unidos (os mais afetados) seguidos de Russia, Reino Unido, Índia, Honk Kong, Alemanha, Indonésia, Irlanda e Holanda

O MANRS descreve quatro ações que os operadores de rede devem tomar:
• Filtragem - Garantir a exatidão de seus próprios anúncios e de anúncios de seus clientes para redes adjacentes
• Anti-spoofing - Habilitar a validação do endereço de origem
• Coordenação - Manter informações de contato atualizadas globalmente acessíveis
• Validação Global - Publicando seus dados, para que outros possam validar informações de roteamento em escala global

As ações do MANRS foram inicialmente projetadas para operadores de rede, mas os Pontos de Troca de Internet (IXPs) também desempenham um papel ativo na proteção da Internet e por isso o MANRS trata especificamente de pontos de troca de trafego.

A MANRS ajuda os IXPs a construir ambientes seguros e demonstram o compromisso do IXP com a segurança e a sustentabilidade do ecossistema da Internet , assim com a melhoria da resiliência do sistema de roteamento.

Peering coordinating fórum

Esta sessão é similiar ao peering fórum do Lacnic, e os IXPs dispõem de bancadas para explicar as suas iniciativas e há uma circulação no salão para ver as ofertas dos diferentes pontos de troca de trafego. O IX.br teve uma bancada no evento e recebeu várias pessoas interessadas em conhecer nossa infraestrutura, ou que já estão presentes em PIX no Brasil.