Simplificar a Internet

1. Antecedentes:

A rápida adoção e a ampla implantação da Internet, que se tornou de facto a espinha dorsal das comunicações a nível mundial, foram acompanhadas de problemas de gravidade variável, desde o assédio cibernético às violações da segurança e ao ransomware. A origem de muitos destes problemas pode ser atribuída à escassez de endereços IPv4.

A igualdade de condições para todos é, desde há muito, uma parte importante da proposta de valor da Internet. No entanto, tal não é uma realidade, mesmo na prática básica de atribuição de endereços. Com base na população mundial [1] e na atual atribuição de endereços IPv4 [2] , os EUA têm 4,91 endereços per capita, enquanto a quota da Zâmbia é de apenas 0,01, um rácio superior a duas ordens e meia de grandeza. A Cidade do Vaticano tem 21,44 endereços per capita, enquanto mais de uma dúzia de entidades do mundo não têm nenhum. Estas discrepâncias gritantes tornam claro que ainda há muito a fazer para atingir o objetivo.

Os esforços para superar as limitações do conjunto de endereços IPv4 levaram ao uso do endereçamento dinâmico, que é fundamentalmente muito mais complexo do que sua contraparte estática. Por alguma razão, os mecanismos dinâmicos continuam a ser usados com o IPv6 na ausência de tais limitações, e ninguém parece questionar a lógica, talvez devido a uma crença ingénua comum de que o endereçamento dinâmico protege a privacidade e a segurança. Na realidade, isso só é verdade com intrusos novatos. O facto é que os criminosos não precisam de saber a identificação específica de uma vítima arbitrária. Por outro lado, ao visar entidades específicas, como escolas, hospitais, empresas, governos, etc., a maioria dos seus endereços IP está prontamente disponível através do serviço DNS (Domain Name System) para facilitar as investigações. Os criminosos mais sérios exploram as fraquezas do sistema escondendo-se atrás de endereços fictícios que podem ser alterados arbitrariamente quando lançam os seus ataques.

Pior ainda, a prática dos endereços dinâmicos tornou tão difícil a realização de análises forenses do tráfego da Internet que justificou a vigilância indiscriminada em massa por parte das forças da ordem para

efeitos de prevenção do crime. Uma vez que não há nada que impeça qualquer outra parte de fazer o mesmo, se assim o desejar, em última análise, resta pouca ou nenhuma privacidade aos indivíduos comuns! Este tema tornou-se bastante controverso e complicado [3] .

Destinado a substituir o melhoramento do IPv4, foi uma grande surpresa o facto de o IPv6 não ser compatível com as versões anteriores, tornando a transição difícil e dispendiosa. Foi necessária a criação do protocolo provisório Dual-Stack [4], que aumentou o custo e não aliviou muito a desvantagem original.

A conetividade extremo-a-extremo sempre foi imposta como o primeiro critério para qualquer proposta de melhoramento da Internet, mas o efeito cumulativo dos desafios acima referidos conduziu a uma CDN (Content Delivery Network - o modelo de funcionamento da Internet atualmente predominante) caracterizada por uma arquitetura mestre-escravo que impede efetivamente a comunicação direta ponto-a-ponto entre utilizadores finais, mesmo no interior de uma comunidade local.

Outra parte da proposta de valor original da Internet era libertar os sistemas de comunicação pública do monopólio de alguns grandes fornecedores de telecomunicações e da regulamentação por parte de agências governamentais. Décadas mais tarde, no entanto, o serviço de Internet está agora segmentado em vários sectores de atividade, cada um deles servido por um único conglomerado multinacional dominante (e alguns concorrentes mais pequenos), que é tão poderoso e influente que consegue fugir às regulamentações, minimizando a responsabilidade pelos problemas que cria.

Simultaneamente, são muitas as críticas ao envolvimento crescente dos governos soberanos de todo o mundo nas operações quotidianas da Internet, que conduzem à fragmentação da Internet numa Splinternet [5]. O facto é que os IAP (fornecedores de acesso à Internet) dividiram a arquitetura da Internet em muitos ASes (sistemas autónomos) [6] que exigem o BGP (Border Gateway Protocol) [7] para os interligar. A Splinternet geopolítica dividiria uma rede de comunicação mundial de camada única em fragmentos nacionais (cerca de 195 no total) [8], enquanto os ASes já criaram camadas (atualmente cerca de 76K e em crescimento) [9] de redes esféricas, cada uma envolvendo todo o globo como uma camada completa de cascas de cebola. Num certo sentido, o número destas camadas

de "Onion-net" é quase duas ordens e meia de grandeza superior ao número de fragmentos potenciais da Splinternet. Este contraste é verdadeiramente espantoso, mesmo antes de reconhecer que o número de ASes possíveis é o mesmo que o conjunto de endereços IPv4 de 32 bits! [10]. Talvez criticar a Splinternet seja uma tática para desviar as atenções da Onion-net.

Se considerarmos tudo o que precede, não é surpreendente que seja necessário tanto tempo para diagnosticar e compreender a extensão de um evento de emergência na Internet, e ainda mais no caso de um hack malicioso - dias, semanas, meses ou mesmo mais tempo - para começar a especular sobre o responsável por um grande ataque cibernético. Em comparação, a PSTN (rede telefónica pública comutada) tradicional é capaz de localizar o autor da chamada mesmo antes de esta ser atendida.

Em resumo, a incapacidade da conceção original da Internet baseada no IPv4 para identificar explícita e inequivocamente cada pessoa no mundo levou a várias soluções dinâmicas. Infelizmente, estas soluções também proporcionaram a camuflagem perfeita para os autores maliciosos que pretendem atacar utilizadores legítimos mas vulneráveis. Embora a nova versão IPv6 tenha endereços mais do que suficientes para identificar todos os IoT (Internet das Coisas), os esquemas provisórios do IPv4 continuam a perpetuar-se. Além disso, a instalação do IPv6, forçada a utilizar o esquema Dual-Stack devido à falta de retrocompatibilidade, é mais complicada e dispendiosa do que o IPv4 puro, o que faz com que as regiões em desenvolvimento tenham dificuldade em adotar o IPv6. Estas complexidades aumentam a vulnerabilidade das redes aos ciberataques. No entanto, está fora de questão uma substituição rápida de qualquer grande sistema de utilização contínua como a Internet, especialmente na sua totalidade.

2. Requisito:

Para contornar este impasse, uma solução realista deve ser capaz de coexistir com o ambiente atual enquanto evolui para um sistema a longo prazo. A abordagem ideal seria introduzir um esquema que se comportasse como parte do sistema existente - sem perturbar as operações em curso - mas que tivesse a capacidade de evoluir para uma rede sobreposta que funcionasse independentemente da instalação de base, mantendo ao mesmo tempo interfaces de comprimento de braço entre as duas para garantir a interoperabilidade e a integridade geral do serviço. Estas evoluiriam gradualmente para dois sistemas que funcionam em paralelo, utilizando a

mesma tecnologia, mas seguindo disciplinas operacionais diferentes para fornecer serviços comparáveis. Isto permitiria aos utilizadores finais experimentarem pessoalmente e compararem os prós e os contras de ambos, de modo a fazerem uma escolha informada da configuração preferida a longo prazo.

3. Solução:

Felizmente, foi identificado um esquema compacto [11] que pode lidar com a maioria das questões discutidas até agora. A abordagem básica deste esquema consiste em utilizar o bloco de rede 240/4 há muito reservado no bloco de construção da CDN existente, CG-NAT (Carrier Grade - Network Address Translation) para estabelecer uma nova instalação, denominada SPR (Semi-Public Router), para sobrepor a atual infraestrutura da Internet. Não é necessária qualquer nova tecnologia no processo desta implantação ao longo do tempo.

Com endereços estáticos suficientes para identificar todos os utilizadores, um SPR não precisa de DHCP (Dynamic Host Configuration Protocol), o que deixa os IAPs sem endereços para atribuir. Com o DNS a degenerar essencialmente numa base de dados quase estática equivalente às páginas brancas da telefonia eletrónica e o AS e o BGP a deixarem de ser necessários, este novo ambiente da Internet é muito simplificado.

Para utilizar o bloco de rede 240/4 que esteve durante tanto tempo com o estatuto de "reservado", pode ser difícil encontrar equipamento facilmente disponível para testar a capacidade do dispositivo e verificar o desempenho da rede. Além disso, esse equipamento deve ser conciso, de baixo custo e com uma curva de aprendizagem mínima, a fim de incentivar o maior número possível de interessados a iniciar esta proposta de transição.

A seguir, descreve-se o equipamento básico e o processo de criação de um banco de ensaio para experiências e demonstrações. As competências e a experiência adquiridas com estas últimas podem depois ser aplicadas para apoiar a implantação efectiva do SPR.

. Terminal Instrumento:

O Xubuntu [12] V18.04.1 foi identificado como o candidato a SO (Sistema Operativo) mais conveniente porque pode assumir dois endereços

IP em simultâneo no mesmo PC portátil anfitrião (Computador Pessoal). Ou seja, cada um desses PCs equipados comporta-se como dois IoTs que partilham a mesma porta de rede de hardware, nomeadamente, um cliente comum endereçado por DHCP juntamente com um cliente estático. Ambos podem assumir o endereço IPv4 familiar ou o endereço 240/4. Um par de IoTs IPv4 DHCP em tais PCs pode estabelecer a conetividade física entre eles através do processo de rede convencional. Em seguida, os IoTs estáticos com endereço 240/4 no mesmo par de PCs podem verificar as caraterísticas de transmissão no ambiente 240/4. Sem alterar qualquer configuração de hardware nem reiniciar os PCs, este teste em duas etapas garante que o meio está pronto para transportar pacotes com qualquer endereço IPv4 em qualquer categoria. Além disso, estes PCs podem ser utilizados com um novo IoT através deste meio para verificar a sua compatibilidade antes de o colocar no terreno.

. Simulador de rede:

Um banco de ensaio compatível com a norma 240/4 serve como tecido de base para qualificar os dispositivos compatíveis e verificar o seu desempenho de transmissão.

A. Para um ponto de partida definitivo, um RG (Routing/Residential Gateway) deve ser totalmente capaz de 240/4 instalando o firmware V19.07.3 do OpenWrt [13], ou superior, que suporta uma longa lista de RGs comerciais. Isso estabelecerá LANs (Local Area Networks) e HANs (Home Area Networks) locais que servem tanto IoTs tradicionais quanto aqueles que assumem endereços 240/4, enquanto se comportam como clientes DHCP 240/4 para a Internet.

B. Para fornecer um tecido de transmissão básico entre instalações (representadas pelos RGs acima) operando como um SPR, o switch gerenciado inteligente D-Link da série DGS-1210 suportado pelo OpenWrt [14] são bons candidatos.

Enquanto um SPR está a ser construído, forma uma rede de sobreposição que serve essencialmente as mesmas instalações com as mesmas funções que o tecido CG-NAT existente, exceto o esquema de encaminhamento predefinido que se torna hierárquico. Este processo pode ser replicado para eventualmente sobrepor um cluster CG-NAT inteiro. Em seguida, vários clusters CG-NAT podem ser servidos a partir de um único

SPR, tirando o máximo partido do tamanho do bloco de rede 240/4, que é 64 vezes superior ao de um bloco de rede 100,64/10, o que estabelece o limite da capacidade de um cluster CG-NAT sem reatribuição dinâmica. Em função da dimensão da população a servir, uma RAN (Regional Area Network) [15] pode ser constituída por um ou mais SPR.

4. Conclusão:

Uma vez que o bloco de rede 240/4 foi formalmente designado como "Reservado para utilização futura" ou "Experimental" durante tantos anos, surgiram naturalmente questões sobre se poderia ser utilizado. Foi noticiado que conglomerados empresariais multinacionais estavam de facto a utilizar o bloco de rede 240/4 para vários fins, sem anúncios [16]. O facto de ter sido necessário algum esforço para descobrir tais actividades indica que a utilização do bloco de rede 240/4 não perturba nem perturbará as operações existentes na Internet. Assim, o bloco de rede 240/4 é um veículo ideal para a implantação do SPR proposto.

Utilizando endereços estáticos, a RAN simplificará o funcionamento da Internet através de um encaminhamento hierárquico que permitirá ao público em geral usufruir de comunicações ponto a ponto, sem o domínio de conglomerados empresariais multinacionais. A natureza estática do esquema de endereçamento permite que a RAN seja mais determinista do que a atual Internet baseada em CDN e, por conseguinte, mais robusta contra ciber-intrusões.

Para mais informações, existe um livro branco em linha [17] que analisa esta proposta de uma perspetiva mais orientada para as empresas.

Referências:

[1] Países do mundo por população;
https://www.worldometers.info/world-population/population-by-country/

[2] Lista de países por atribuição de endereços IPv4:
https://en.wikipedia.org/wiki/List_of_countries_by_IPv4_address_allocation

[3] Estado de vulnerabilidade da cibersegurança
https://blog.apnic.net/2021/02/03/the-internet-of-trash/

[4] IPv6:
https://en.wikipedia.org/wiki/IPv6

[5] Splinternet
https://en.wikipedia.org/wiki/Splinternet#:~:text=The%20splinternet%20(também%20referido%20como,religião%2C%20e%20interesses%20nacionais%20divergentes.

[6] Sistema Autónomo
https://en.wikipedia.org/wiki/Autonomous_system_(Internet)

[7] Protocolo de Gateway de Fronteira
https://en.wikipedia.org/wiki/Border_Gateway_Protocol

[8] Países do mundo
https://www.worldometers.info/geography/how-many-countries-are-there-in-the-world/#:~:text=There%20are%20195%20countries%20in,and%20the%20State%20of%20Palestine.

[9] Número de ASes actuais
https://thyme.apnic.net/current/data-summary

[10] Números de sistemas autónomos
https://www.arin.net/resources/guide/asn/

[11] Patente dos EUA n.º 11.159.425
https://image-ppubs.uspto.gov/dirsearch-public/print/downloadPdf/11159425

[12] Xubuntu
https://xubuntu.org/

[13] OpenWrt
https://openwrt.org/toh/start?toh.filter.supportedcurrentrel=22.03%7C23.05

[14] Switches inteligentes da série D-Link DGS-1210
https://www.dlink.com/us/en/products/dgs-1210-series-gigabit-smart-plus-switches

[15] Simulador de redes de área regional
https://www.avinta.com/gallery/RegionalAreaNetworkSimulator.pdf

[16] Utilização de 240/4 sem aviso prévio
https://labs.ripe.net/author/qasim-lone/2404-as-seen-by-ripe-atlas/

[17] Renovar a Internet:
https://www.avinta.com/gallery/RevampTheInternet.pdf

Terminologia, abreviatura e acrónimo:

. AS: Sistema Autónomo

. BGP: Border Gateway Protocol

. CDN:Rede de distribuição de conteúdos

. CG-NAT: Tradução de endereços de rede de nível de operadora

. DHCP: Protocolo de Configuração Dinâmica de Anfitrião

. DNS: Sistema de Nomes de Domínio

. Dual-Stack: Um ambiente de rede que suporta a utilização simultânea de endereços IPv4 e IPv6.

. HAN: Home Area Network (rede no local para particulares/residências)

. IAP: fornecedor de acesso à Internet

. IoT: Internet of Thing (Internet das coisas) .

. IPv4: Protocolo Internet versão 4

. IPv6: Protocolo Internet versão 6

. LAN: Local Area Network (rede local utilizada pelas instituições)

. OS: Sistema Operativo

. PC: Computador pessoal

. PSTN: Rede telefónica pública comutada

. RAN: Rede regional

. RG: Encaminhamento/Gateways residenciais

. SPR: Semi-Public Router

. 240/4 Netblock: Conjunto de endereços IPv4 que vai de 240.0.0.0 a 255.255.255.255, totalizando cerca de 256 milhões (256M) ou um quarto de bilião (0.256B) de endereços que não estão a ser usados formalmente desde 1981-09 porque foram designados como "Experimentais" ou "Reservados" para "Uso futuro".

https://www.iana.org/assignments/ipv4-address-space/ipv4-address-space.xhtml