Racionalizar Internet

1. Antecedentes:

La rápida adopción y el amplio despliegue de Internet para convertirse en la espina dorsal de facto de las comunicaciones mundiales han ido acompañados de problemas de diversa gravedad, desde el ciberacoso a las brechas de seguridad, pasando por el ransomware. Muchos de estos problemas tienen su origen en la escasez de direcciones IPv4.

La igualdad de condiciones para todos ha sido durante mucho tiempo una parte importante de la propuesta de valor de Internet. Sin embargo, esto no es una realidad ni siquiera en la práctica básica de asignación de direcciones. Teniendo en cuenta la población mundial [1] y la asignación actual de IPv4 [2] , EE.UU. tiene 4,91 direcciones per cápita, mientras que la cuota de Zambia es de sólo 0,01, una proporción superior a dos órdenes y medio de magnitud. La Ciudad del Vaticano tiene 21,44 per cápita, mientras que más de una docena de entidades del mundo no tienen ninguna. Estas marcadas discrepancias dejan claro que aún queda mucho por hacer para alcanzar el objetivo.

Los esfuerzos por superar las limitaciones del conjunto de direcciones IPv4 llevaron al uso del direccionamiento dinámico, que es fundamentalmente mucho más complicado que su homólogo estático. Por alguna razón, los mecanismos dinámicos siguen utilizándose con IPv6 en ausencia de tales limitaciones, y nadie parece cuestionar su razón de ser, quizás debido a la creencia ingenua común de que el direccionamiento dinámico protege la privacidad y la seguridad. En realidad, esto resulta ser cierto sólo con intrusos novatos. El hecho es que los agresores no necesitan conocer la identificación específica de una víctima arbitraria. Por otro lado, cuando se dirigen a entidades específicas como escuelas, hospitales, empresas, gobiernos, etc., la mayoría de sus direcciones IP están fácilmente disponibles a través del servicio DNS (Sistema de Nombres de Dominio) para facilitar las consultas. Los delincuentes serios explotan las debilidades del sistema escondiéndose tras direcciones ficticias que pueden cambiar arbitrariamente cuando lanzan sus ataques.

Peor aún, la práctica de las direcciones dinámicas ha dificultado tanto los análisis forenses del tráfico de Internet que ha justificado la vigilancia masiva indiscriminada por parte de las fuerzas del orden en aras de la

prevención del delito. Como no hay nada que impida a los demás hacer lo mismo, si así lo desean, en última instancia, ¡poca o ninguna privacidad queda para el ciudadano de a pie! Esto se ha convertido en un tema bastante controvertido y enrevesado [3] .

Previsto como sustituto para mejorar IPv4, fue una gran sorpresa que IPv6 resultara no ser compatible con versiones anteriores, lo que supuso una transición difícil y costosa. Fue necesaria la creación del protocolo provisional Dual-Stack [4], que incrementó los costes sin aliviar realmente gran parte de la desventaja original.

La conectividad de extremo a extremo siempre se ha impuesto como primer criterio en cualquier propuesta de mejora de Internet, pero el efecto acumulativo de los retos anteriores ha dado lugar a una CDN (Red de Entrega de Contenidos, el modelo de funcionamiento de Internet predominante en la actualidad) caracterizada por una arquitectura maestro-esclavo que, de hecho, impide la comunicación directa de igual a igual entre usuarios finales, incluso dentro de una comunidad local.

Otra parte de la propuesta de valor original de Internet era liberar los sistemas públicos de comunicación del monopolio de unos pocos grandes proveedores de telecomunicaciones y de la regulación de los organismos gubernamentales. Décadas más tarde, sin embargo, el servicio de Internet está segmentado en varios sectores empresariales, cada uno de ellos atendido por un único conglomerado multinacional dominante (y unos pocos competidores más pequeños) que es tan poderoso e influyente que es capaz de eludir la normativa al tiempo que resta importancia a la responsabilidad por los problemas que crea.

Al mismo tiempo, se critica mucho la creciente implicación de gobiernos soberanos de todo el mundo en las operaciones diarias de Internet, ya que conduce a la fragmentación de Internet en una Splinternet [5]. El hecho es que los IAP (Proveedores de Acceso a Internet) han dividido la arquitectura de Internet en muchos AS (Sistemas Autónomos) [6] que requieren BGP (Protocolo de Pasarela Fronteriza) [7] para interconectarlos. La Splinternet geopolítica dividiría una red de comunicación mundial de una sola capa en fragmentos nacionales (en total unos 195) [8], mientras que los ASes ya han creado capas (actualmente unas 76K y creciendo) [9] de redes esféricas, cada una de las cuales envuelve todo el globo como una capa completa de cáscaras de cebolla. En cierto sentido, el número de estas capas

"Onion-net" es casi dos órdenes y medio de magnitud mayor que el de los fragmentos potenciales de Splinternet. Este contraste es realmente alucinante, ¡incluso antes de reconocer que el número de posibles AS es el mismo que el conjunto de direcciones IPv4 de 32 bits! [10]. Tal vez criticar la Splinternet sea una táctica para distraer la atención y no centrarse en la Onion-net.

Si se tiene en cuenta todo lo anterior, no es de extrañar que se necesite tanto tiempo para diagnosticar y comprender el alcance de un suceso de emergencia en Internet, y aún más en el caso de un pirateo malicioso -días, semanas, meses o incluso más tiempo- para empezar a especular sobre la parte que está detrás de un ciberataque importante. En comparación, la RTPC (Red Telefónica Pública Conmutada) tradicional es capaz de localizar a la persona que llama incluso antes de que se conteste la llamada.

En resumen, la incapacidad del diseño original de Internet basado en IPv4 para identificar de forma explícita y única a todas las personas del mundo dio lugar a diversos remedios dinámicos. Por desgracia, estos remedios también proporcionaron el camuflaje perfecto para los autores maliciosos que pretendían atacar a usuarios legítimos pero vulnerables. Aunque la nueva versión IPv6 dispone de direcciones más que suficientes para identificar a todos los IoT (Internet de las cosas), los esquemas provisionales de IPv4 siguen perpetuándose. Además, la instalación de IPv6, obligada a utilizar el esquema Dual-Stack por falta de compatibilidad con versiones anteriores, es más complicada y cara que la de IPv4 puro, con lo que las regiones en desarrollo tienen dificultades para adoptar IPv6. Estas complejidades aumentan la vulnerabilidad de la red a los ciberataques. No obstante, una sustitución rápida de cualquier gran sistema de uso continuo como Internet, sobre todo en su totalidad, está fuera de lugar.

2. Requisito:

Para sortear este impasse, una solución realista debe ser capaz de coexistir con el entorno actual al tiempo que evoluciona hacia un sistema a largo plazo. Lo ideal sería introducir un sistema que se comportara como parte del actual -sin perturbar las operaciones en curso- pero que pudiera evolucionar hacia una red superpuesta que funcionara independientemente de la instalación de base, manteniendo al mismo tiempo interfaces entre ambas para garantizar la interoperabilidad y la integridad general del servicio. Estos sistemas evolucionarían gradualmente hasta convertirse en

dos sistemas que funcionarían en paralelo, utilizando la misma tecnología, pero siguiendo disciplinas operativas diferentes para prestar servicios comparables. Esto permitiría a los usuarios finales experimentar personalmente y comparar los pros y los contras de ambos para elegir con conocimiento de causa la configuración preferida a largo plazo.

3. Solución:

Afortunadamente, se ha identificado un esquema compacto [11] que puede resolver la mayoría de los problemas discutidos hasta ahora. El enfoque básico de este esquema es utilizar el bloque de red 240/4 reservado durante mucho tiempo en el bloque de construcción de la CDN existente, CG-NAT (Carrier Grade - Network Address Translation) para establecer una nueva instalación, denominada SPR (Semi-Public Router), que se superponga a la infraestructura actual de Internet. No se requiere ninguna nueva tecnología en el proceso de despliegue a lo largo del tiempo.

Al disponer de suficientes direcciones estáticas para identificar a cada usuario, un SPR no necesita DHCP (Dynamic Host Configuration Protocol), lo que deja a los IAP sin direcciones asignadas que asignar. Como el DNS degenera esencialmente en una base de datos casi estática equivalente a las Páginas Blancas de la telefonía electrónica y ya no se necesitan AS ni BGP, este nuevo entorno de Internet se simplifica mucho.

Para utilizar el bloque de red 240/4 que ha estado en estado "Reservado" durante tanto tiempo, puede ser difícil encontrar equipos fácilmente disponibles para probar la capacidad del dispositivo y verificar el rendimiento de la red. Además, dicho dispositivo debe ser conciso, de bajo coste y con una curva de aprendizaje mínima para animar al mayor número posible de interesados a poner en marcha esta transición propuesta.

A continuación se describen el equipo y el proceso básicos para montar un banco de pruebas para experimentos y demostraciones. Los conocimientos y la experiencia adquiridos en estos últimos pueden aplicarse después para ayudar al despliegue real del SPR.

. Terminal Instrumento:

Xubuntu [12] V18.04.1 ha sido identificado como el candidato de SO (Sistema Operativo) más conveniente porque puede asumir direcciones IP

duales simultáneamente en el mismo PC portátil anfitrión (Ordenador Personal). Es decir, cada uno de estos PC equipados se comporta como dos IoT que comparten el mismo puerto de red de hardware, a saber, un cliente común con dirección DHCP junto a otro estático. Ambos pueden asumir la conocida dirección IPv4 o la 240/4. Un par de IOs IPv4 DHCP en dichos PCs pueden establecer la conectividad física entre ellos mediante el proceso de red convencional. A continuación, los IoT estáticos con dirección 240/4 en el mismo par de PC pueden verificar las características de transmisión en el entorno 240/4. Sin cambios en ninguna configuración de hardware ni reinicio de los PC, esta prueba en dos pasos garantiza que el medio está preparado para transportar paquetes con cualquier dirección IPv4 en cualquiera de las dos categorías. Además, estos PC pueden utilizarse con un nuevo IoT a través de este medio para verificar su compatibilidad antes de desplegarlo sobre el terreno.

. **Simulador de red:**

Un banco de pruebas compatible con 240/4 sirve de tejido básico para calificar los dispositivos compatibles y comprobar sus prestaciones de transmisión.

A. Para un punto de partida definitivo, un RG (Routing/Residential Gateway) debería ser totalmente capaz de 240/4 instalando OpenWrt [13] firmware V19.07.3, o superior, que soporta una larga lista de RGs comerciales. Esto establecerá LANs (Redes de Área Local) y HANs (Redes de Área Doméstica) locales que sirvan tanto a IoTs tradicionales como a aquellos que asuman direcciones 240/4, a la vez que se comportan como clientes DHCP 240/4 para Internet.

B. Para proporcionar un tejido de transmisión básico entre locales (representados por los RGs anteriores) operando como un SPR, los switches gestionados inteligentes D-Link Serie DGS-1210 soportados por OpenWrt [14] son buenos candidatos.

Mientras se construye una SPR, se forma una red superpuesta que sirve esencialmente a las mismas instalaciones con las mismas funciones que el tejido CG-NAT existente, excepto que el esquema de enrutamiento por defecto se vuelve jerárquico. Este proceso puede repetirse para acabar superponiéndose a todo un clúster CG-NAT. A continuación, se puede dar servicio a varios clusters CG-NAT desde un único SPR aprovechando al

máximo el tamaño del netblock de 240/4, que es 64 veces mayor que el de un netblock de 100,64/10, que establece el límite de la capacidad de un cluster CG-NAT sin reasignación dinámica. Dependiendo del tamaño de la población a la que se preste servicio, una RAN (Red de Área Regional) [15] puede constar de una o más SPR.

4. Conclusión:

Dado que el bloque de red 240/4 se ha designado formalmente como "Reservado para uso futuro" o "Experimental" durante tantos años, surgieron naturalmente preguntas sobre si se podía utilizar. Se ha informado de que conglomerados empresariales multinacionales están utilizando realmente el bloque de red 240/4 para diversos fines sin anunciarlo [16]. El hecho de que haya costado cierto esfuerzo descubrir tales actividades indica que el uso del bloque de red 240/4 no perturba ni perturbará las operaciones existentes en Internet. Así pues, el bloque de red 240/4 es un vehículo ideal para desplegar el SPR propuesto.

Mediante el uso de direcciones estáticas, la RAN agilizará el funcionamiento de Internet a través de un enrutamiento jerárquico que permitirá al público en general disfrutar de la comunicación entre iguales, libre del dominio de los conglomerados empresariales multinacionales. La naturaleza estática del esquema de direccionamiento permite a la RAN ser más determinista que la actual Internet basada en CDN y, por tanto, más robusta contra las intrusiones cibernéticas.

Para más información, existe un libro blanco en línea [17] que analiza esta propuesta desde una perspectiva más empresarial.

Referencias:

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

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

[3] Estado de vulnerabilidad de la ciberseguridad https://blo.apnic.net/2021/02/03/la-internet-de-la-basura/

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

[5] Splinternet
https://en.wikipedia.org/wiki/Splinternet#:~:text=The%20splinternet%20(also%20referred%20to,religion%2C%20and%20divergent%20national%20interests.

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

[7] Protocolo de pasarela fronteriza
https://en.wikipedia. o rg/wiki/Border_Gateway_Protocolo

[8] Países del 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 AS actuales
https://thyme.apnic.net/current/data-summary

[10] Números de sistema autónomo
https://www.arin.net/resources/guide/asn/

[11] Patente estadounidense nº 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 de la serie D-Link DGS-1210
https://www.dlink.com/us/en/products/dgs-1210-series-gigabit-smart-plus-switches

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

[16] Uso de 240/4 sin previo aviso
https://labs.ripe.net/author/qasim-lone/2404-as-seen-by-ripe-atlas/

[17] Revamp The Internet:
https://www.avinta.com/gallery/RevampTheInternet.pdf

Terminología, abreviatura y acrónimo:

. AS: Sistema Autónomo

. BGP: Protocolo de Pasarela Fronteriza

. CDN: Red de distribución de contenidos

. CG-NAT: Traducción de direcciones de red de nivel de operador

. DHCP: Protocolo de configuración dinámica de host

. DNS: Sistema de nombres de dominio

. Dual-Stack: Entorno de red que admite el uso simultáneo de direcciones IPv4 e IPv6.

. HAN: Home Area Network (Red localpara particulares/ residencias)

. IAP: Proveedor de acceso a Internet

. IoT: Internet de las Cosas

. IPv4: Protocolo de Internet versión 4

. IPv6: Protocolo Internet versión 6

. LAN: Local Area Network (Red local utilizada por las instituciones)

. SO: Sistema operativo

. PC: Ordenador personal

. PSTN: Red Telefónica Pública Conmutada

. RAN: Red de Área Regional

. RG: Enrutamiento/Pasarelas residenciales

. SPR: Router semipúblico

. 240/4Netblock: Conjunto de direcciones IPv4 comprendidas entre 240.0.0.0 y 255.255.255.255, que suman aproximadamente 256 millones (256M) o un cuarto de billón (0.256B) de direcciones que no se utilizan formalmente desde 1981-09 porque se designaron como "Experimentales" o "Reservadas" para "Uso futuro".

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