Das Internet rationalisieren

1. Hintergrund:

Die rasche Annahme und weite Verbreitung des Internets, das sich de facto zum weltweiten Kommunikations-Backbone entwickelt hat, wurde von Problemen begleitet, die von Cyber-Belästigung über Sicherheitsverletzungen bis hin zu Ransomware reichen. Viele dieser Probleme lassen sich auf die Knappheit des IPv4-Adresspools zurückführen.

Gleiche Wettbewerbsbedingungen für alle sind seit langem ein wichtiger Teil des Wertversprechens des Internets. Dies ist jedoch nicht einmal in der grundlegenden Praxis der Adressenzuweisung Realität. Auf der Grundlage der Weltbevölkerung [1] und der aktuellen IPv4-Zuteilung [2] verfügen die USA über 4,91 Adressen pro Kopf, während der Anteil Sambias nur 0,01 beträgt - ein Verhältnis von mehr als zweieinhalb Größenordnungen. Die Vatikanstadt hat 21,44 Adressen pro Kopf, während mehr als ein Dutzend Entitäten in der Welt keine haben. Diese krassen Diskrepanzen machen deutlich, dass noch viel zu tun bleibt, um das Ziel zu erreichen.

Die Bemühungen, die Beschränkungen des IPv4-Adresspools zu überwinden, führten zur Verwendung der dynamischen Adressierung, die grundsätzlich viel aufwendiger ist als ihr statisches Gegenstück. Aus irgendeinem Grund werden bei IPv6 weiterhin dynamische Mechanismen verwendet, obwohl es keine derartigen Beschränkungen gibt, und niemand scheint die Gründe dafür in Frage zu stellen, vielleicht aufgrund des weit verbreiteten naiven Glaubens, dass die dynamische Adressierung die Privatsphäre und die Sicherheit schützt. In Wirklichkeit trifft dies aber nur auf unerfahrene Eindringlinge zu. Tatsache ist, dass die Täter die spezifische Identifizierung eines beliebigen Opfers nicht kennen müssen. Wenn es jedoch um bestimmte Einrichtungen wie Schulen, Krankenhäuser, Unternehmen, Regierungen usw. geht, sind die meisten ihrer IP-Adressen über den DNS-Dienst (Domain Name System) leicht zugänglich und erleichtern die Nachforschungen. Seriöse Täter nutzen die Schwächen des Systems aus, indem sie sich hinter fiktiven Adressen verstecken, die bei ihren Angriffen beliebig geändert werden können.

Schlimmer noch, die Praxis der dynamischen Adressen hat die Durchführung forensischer Analysen des Internetverkehrs so erschwert, dass

sie eine wahllose Massenüberwachung durch die Strafverfolgungsbehörden zur Verbrechensverhütung rechtfertigt. Da es nichts gibt, was andere Parteien davon abhalten könnte, das Gleiche zu tun, wenn sie dazu in der Lage sind, bleibt letztlich wenig oder gar keine Privatsphäre für den normalen Bürger übrig! Dies ist ein ziemlich kontroverses und verworrenes Thema geworden [3] .

Als Ersatz für die Verbesserung von IPv4 gedacht, stellte sich überraschend heraus, dass IPv6 nicht abwärtskompatibel war, was einen schwierigen und kostspieligen Übergang zur Folge hatte. Dies machte die Schaffung des vorläufigen Dual-Stack-Protokolls [4] erforderlich, das die Kosten in die Höhe trieb, ohne das ursprüngliche Handicap wirklich zu beheben.

Die End-to-End-Konnektivität wurde immer als erstes Kriterium für alle vorgeschlagenen Internet-Verbesserungen vorgeschrieben, aber die kumulative Wirkung der oben genannten Herausforderungen hat zu einem CDN (Content Delivery Network - das derzeit vorherrschende Internet-Betriebsmodell) geführt, das durch eine Master-Slave-Architektur gekennzeichnet ist, die eine direkte Peer-to-Peer-Kommunikation zwischen den Endnutzern verhindert, selbst innerhalb einer lokalen Gemeinschaft.

Ein weiterer Teil des ursprünglichen Wertversprechens des Internets bestand darin, die öffentlichen Kommunikationssysteme von der Monopolisierung durch einige wenige große Telekommunikationsanbieter und von der Regulierung durch staatliche Stellen zu befreien. Jahrzehnte später sind die Internetdienste jedoch in mehrere Geschäftsbereiche aufgeteilt, die jeweils von einem einzigen dominanten multinationalen Konzern (und einigen kleineren Konkurrenten) bedient werden, der so mächtig und einflussreich ist, dass er sich den Vorschriften entziehen und die Verantwortung für die von ihm verursachten Probleme herunterspielen kann.

Gleichzeitig gibt es viel Kritik an der zunehmenden Einmischung souveräner Regierungen weltweit in den täglichen Internetbetrieb, die zu einer Fragmentierung des Internets in ein Splinternet führt [5]. Tatsache ist, dass die IAPs (Internet Access Providers) die Internet-Architektur in viele ASes (Autonomous Systems) aufgeteilt haben [6] und BGP (Border Gateway Protocol) [7] benötigen, um diese miteinander zu verbinden. Das geopolitische Splinternet würde ein einlagiges weltweites

Kommunikationsnetz in nationale Fragmente (insgesamt etwa 195) unterteilen [8], während die ASes bereits Schichten (derzeit etwa 76K, Tendenz steigend) [9] von kugelförmigen Netzen geschaffen haben, die jeweils den gesamten Globus wie eine komplette Schicht von Zwiebelschalen umhüllen. In gewissem Sinne ist die Anzahl dieser "Zwiebelnetz"-Schichten um fast zweieinhalb Größenordnungen größer als die der potenziellen Splinternet-Fragmente. Dieser Kontrast ist wirklich verblüffend, selbst wenn man bedenkt, dass die Anzahl der möglichen AS die gleiche ist wie der 32-Bit-IPv4-Adressenpool! [10]. Vielleicht ist die Kritik am Splinternet eine Taktik, um die Aufmerksamkeit von der Konzentration auf das Onion-Netz abzulenken.

Wenn man all das zusammennimmt, ist es nicht verwunderlich, dass so viel Zeit benötigt wird, um das Ausmaß eines Internet-Notfalls zu diagnostizieren und zu verstehen, und noch mehr im Falle eines böswilligen Hacks - Tage, Wochen, Monate oder sogar länger -, um nur ansatzweise über die Partei hinter einem großen Cyberangriff zu spekulieren. Im Vergleich dazu ist das herkömmliche PSTN (Public Switched Telephone Network) in der Lage, den Anrufer zu lokalisieren, noch bevor ein Anruf entgegengenommen wird.

Zusammenfassend lässt sich sagen, dass die Unfähigkeit des ursprünglichen IPv4-basierten Internetentwurfs, jede Person auf der Welt explizit und eindeutig zu identifizieren, zu verschiedenen dynamischen Abhilfemaßnahmen führte. Leider boten diese Abhilfemaßnahmen auch die perfekte Tarnung für böswillige Täter, die legitime, aber anfällige Nutzer angreifen wollten. Obwohl die neue Version IPv6 über mehr als genug Adressen verfügt, um alle IoT-Geräte (Internet der Dinge) zu identifizieren, werden die IPv4-Interimsregelungen weiterhin aufrechterhalten. Darüber hinaus ist die IPv6-Einrichtung, die aufgrund der fehlenden Abwärtskompatibilität zur Verwendung des Dual-Stack-Schemas gezwungen ist, komplizierter und teurer als reines IPv4, was dazu führt, dass sich die Entwicklungsregionen schwer tun, IPv6 zu übernehmen. Diese Komplexität erhöht die Anfälligkeit des Netzes für Cyberangriffe. Eine schnelle Ablösung eines kontinuierlich genutzten Großsystems wie des Internets, insbesondere in seiner Gesamtheit, kommt jedoch nicht in Frage.

2. Anforderung:

Um diese Pattsituation zu umgehen, muss eine realistische Lösung in der Lage sein, mit dem derzeitigen Umfeld zu koexistieren und sich gleichzeitig zu einem langfristigen System zu entwickeln. Der ideale Ansatz wäre die Einführung eines Systems, das sich wie ein Teil des bestehenden Systems verhält - ohne Unterbrechung des laufenden Betriebs -, das aber die Möglichkeit hat, sich zu einem Overlay-Netz zu entwickeln, das unabhängig von der Basiseinrichtung funktioniert, wobei die Schnittstellen zwischen den beiden Systemen zur Gewährleistung der Interoperabilität und der allgemeinen Dienstintegrität auf Armeslänge beibehalten werden. Diese würden sich allmählich zu zwei parallel arbeitenden Systemen entwickeln, die dieselbe Technologie nutzen, aber unterschiedlichen Betriebsdisziplinen folgen, um vergleichbare Dienste bereitzustellen. Dies würde die Endnutzer in die Lage versetzen, persönlich zu experimentieren und die Vor- und Nachteile beider Systeme zu vergleichen, um eine fundierte Entscheidung für die bevorzugte langfristige Konfiguration zu treffen.

3. Lösung:

Glücklicherweise wurde ein kompaktes Schema [11] gefunden, das die meisten der bisher diskutierten Probleme lösen kann. Der grundlegende Ansatz dieses Konzepts besteht darin, den seit langem reservierten Netzblock 240/4 im bestehenden CDN-Baustein CG-NAT (Carrier Grade - Network Address Translation) für die Einrichtung einer neuen Einrichtung namens SPR (Semi-Public Router) zu nutzen, die die aktuelle Internet-Infrastruktur überlagert. Für eine derartige Einrichtung ist keine neue Technologie erforderlich.

Da ein SPR über genügend statische Adressen zur Identifizierung jedes Benutzers verfügt, benötigt es kein DHCP (Dynamic Host Configuration Protocol), so dass IAPs keine Adressen mehr zuweisen müssen. Da DNS im Wesentlichen zu einer quasi-statischen Datenbank degeneriert, die den elektronischen Telefonbüchern entspricht, und AS und BGP nicht mehr benötigt werden, ist diese neue Internet-Umgebung sehr viel einfacher.

Für die Nutzung des 240/4-Netzblocks, der schon so lange "reserviert" ist, könnte es schwierig sein, leicht verfügbare Geräte zum Testen der Gerätefähigkeit und zur Überprüfung der Netzleistung zu finden. Außerdem muss eine solche Einrichtung übersichtlich, kostengünstig und mit

minimaler Lernkurve sein, um möglichst viele Interessenten zu ermutigen, den vorgeschlagenen Übergang einzuleiten.

Im Folgenden werden die Grundausstattung und das Verfahren zur Einrichtung eines Prüfstands für Experimente und Demonstrationen beschrieben. Die dabei gewonnenen Fähigkeiten und Erfahrungen können dann zur Unterstützung der eigentlichen SPR-Einführung genutzt werden.

. **Terminal Instrument:**

Xubuntu [12] V18.04.1 wurde als der geeignetste Kandidat für ein Betriebssystem identifiziert, weil es zwei IP-Adressen gleichzeitig auf demselben Host-Notebook-PC (Personal Computer) annehmen kann. Das heißt, jeder so ausgestattete PC verhält sich wie zwei IoTs, die sich denselben Hardware-Netzwerkanschluss teilen, nämlich ein gemeinsamer DHCP-adressierter Client neben einem statischen. Beide können entweder die bekannte IPv4- oder die 240/4-Adresse annehmen. Ein Paar von IPv4-DHCP-IoTs auf solchen PCs kann die physische Konnektivität zwischen ihnen über den herkömmlichen Netzwerkprozess herstellen. Anschließend können die statischen IoTs mit 240/4-Adressen auf demselben PC-Paar die Übertragungseigenschaften in der 240/4-Umgebung überprüfen. Ohne Änderungen an der Hardware-Einrichtung und ohne Neustart der PCs stellt dieser zweistufige Test sicher, dass das Medium für die Übertragung von Paketen mit beliebigen IPv4-Adressen in beiden Kategorien bereit ist. Darüber hinaus können diese PCs mit einem neuen IoT über dieses Medium verwendet werden, um dessen Kompatibilität zu überprüfen, bevor es im Feld eingesetzt wird.

. **Netzwerk-Simulator:**

Ein 240/4-kompatibler Prüfstand dient als Grundgerüst für die Qualifizierung kompatibler Geräte und die Überprüfung ihrer Übertragungsleistung.

A. Als definitiver Ausgangspunkt sollte ein RG (Routing/Residential Gateway) durch Installation der OpenWrt [13] Firmware V19.07.3 oder höher, die eine lange Liste kommerzieller RGs unterstützt, vollständig 240/4-fähig gemacht werden. Dadurch werden lokale LANs (Local Area Networks) und HANs (Home Area Networks) eingerichtet, die sowohl traditionelle IoTs als auch solche, die 240/4-

Adressen annehmen, bedienen und sich gegenüber dem Internet wie 240/4-DHCP-Clients verhalten.

B. Für die Bereitstellung einer grundlegenden Übertragungsstruktur zwischen Räumlichkeiten (dargestellt durch die oben genannten RGs), die als SPR betrieben werden, sind die OpenWrt-unterstützten D-Link Smart Managed Switches der DGS-1210-Serie [14] gute Kandidaten.

Während ein SPR ausgebaut wird, bildet es ein Overlay-Netz, das im Wesentlichen dieselben Räumlichkeiten mit denselben Funktionen wie die bestehende CG-NAT-Struktur bedient, mit der Ausnahme, dass das Standard-Routing-Schema hierarchisch wird. Dieser Prozess kann repliziert werden, um schließlich einen ganzen CG-NAT-Cluster zu überlagern. Als nächstes können mehrere CG-NAT-Cluster von einem einzigen SPR aus bedient werden, indem die Größe des 240/4-Netzblocks voll ausgenutzt wird, die 64-mal so groß ist wie die eines 100,64/10-Netzblocks, der die Kapazitätsgrenze eines CG-NAT-Clusters ohne dynamische Neuzuweisung darstellt. Je nach Größe der zu versorgenden Bevölkerung kann ein RAN (Regional Area Network) [15] aus einem oder mehreren SPRs bestehen.

4. Schlussfolgerung:

Da der 240/4-Netzblock seit vielen Jahren offiziell als "Reserviert für zukünftige Nutzung" oder "Experimentell" bezeichnet wird, kamen natürlich Fragen auf, ob er genutzt werden kann. Es wurde berichtet, daß multinationale Firmenkonglomerate den Netzblock 240/4 tatsächlich für verschiedene Zwecke nutzen, ohne dies anzukündigen [16]. Die Tatsache, daß es einiger Anstrengungen bedurfte, um solche Aktivitäten zu entdecken, zeigt, daß die Nutzung des Netzblocks 240/4 den bestehenden Internetbetrieb nicht stört und auch nicht stören wird. Der 240/4-Netzblock ist also ein ideales Vehikel für den Einsatz der vorgeschlagenen SPR.

Durch die Verwendung statischer Adressen wird das RAN den Internetbetrieb über eine hierarchische Leitweglenkung rationalisieren, die der Allgemeinheit eine Peer-to-Peer-Kommunikation ermöglicht, die nicht mehr von multinationalen Unternehmenskonglomeraten beherrscht wird. Die statische Natur des Adressierungsschemas ermöglicht es dem RAN, deterministischer zu sein als das bestehende CDN-basierte Internet und somit robuster gegen Cyberangriffe.

Für weitere Informationen gibt es ein Online-Whitepaper [17], in dem dieser Vorschlag aus einer eher geschäftsorientierten Perspektive analysiert wird.

Referenzen:

[1] Länder der Welt nach Bevölkerung; https://www.worldometers.info/world-population/population-by-country/

[2] Liste der Länder nach IPv4-Adresszuweisung: https://en.wikipedia.org/wiki/List_of_countries_by_IPv4_address_allocation

[3] Status der Cybersicherheitslücken _ghttps://blo.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(also%20referred%20to,religion%2C%20and%20divergent%20national%20interests.

[6] Autonomes System https://en.wikipedia.org/wiki/Autonomous_system_(Internet)

[7] Border Gateway Protokoll https://en.wikipedia. o rg/wiki/Grenzübergangsprotokoll

[8] Länder der Welt 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] Anzahl der aktuellen ASes https://thyme.apnic.net/current/data-summary

[10] Autonome System-Nummern
https://www.arin.net/resources/guide/asn/

[11] US-Patent Nr. 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] D-Link DGS-1210 Serie Smart Switches
https://www.dlink.com/us/en/products/dgs-1210-series-gigabit-smart-plus-switches

[15] Regional Area Network Simulator
https://www.avinta.com/gallery/RegionalAreaNetworkSimulator.pdf

[16] Unangekündigte Verwendung von 240/4
https://labs.ripe.net/author/qasim-lone/2404-as-seen-by-ripe-atlas/

[17] Das Internet neu gestalten:
https://www.avinta.com/gallery/RevampTheInternet.pdf

Terminologie, Abkürzungen und Akronyme:

. AS: Autonomes System

. BGP: Gateway Protokoll

. CDN: Content Delivery Network

. CG-NAT: Carrier Grade Network Address Translation

. DHCP: Dynamisches Host-Konfigurationsprotokoll

. DNS: Domänennamen-System

. Dual-Stack: Eine Netzwerkumgebung, die die gleichzeitige Verwendung von IPv4- und IPv6-Adressen unterstützt.

. HAN: Home Area Netzwerk (Vor-Ort-Netzfür Privatpersonen/Wohnungen)

. IAP: Internet-Zugangsanbieter

. IoT: Internet der Dinge

. IPv4: Internetprotokoll Version 4

. IPv6: Internetprotokoll Version 6

. LAN: Lokales Netzwerk (von den Institutionen genutztes lokales Netzwerk)

. OS: Betriebssystem

. PC: Personal Computer

PSTN: Öffentliches Telefonnetz

. RAN: Regional Area Network

. RG: Routing/Residential Gateways

. SPR: Semi-Public Router

. 240/4Netblock: IPv4-Adressenpool im Bereich von 240.0.0.0 bis 255.255.255.255, der etwa 256 Millionen (256M) oder eine Viertelmilliarde (0.256B) Adressen umfasst, die seit 1981-09 nicht mehr offiziell verwendet werden, weil sie als "experimentell" oder "reserviert" für "zukünftige Verwendung" eingestuft wurden.

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