インターネットを合理化する

1. 背景:

事実上の世界的な通信バックボーンとなるインターネットの急速な普及と広範な展開には、サイバーハラスメントからセキュリティ侵害、ランサムウェアに至るまで、深刻度の異なる問題が伴いました。これらの問題の多くの原因は、IPv4 アドレス プールの不足にあると考えられます。

すべての人にとって平等な競争の場は、長い間、インターネットの価値提案の大きな部分を占めてきました。しかし、これは基本的なアドレス割り当ての実践においてさえ現実的ではありません。世界の人口 [1] と現在の IPv4 割り当て [2] に基づくと、米国は 1 人当たり 4.91 個のアドレスを持っていますが、ザンビアのシェアはわずか 0.01 であり、その比率は 2.5 桁を超えています。バチカン市国には 1 人当たり 21.44 人がいますが、世界の十数団体には 1 人もいません。これらの明らかな矛盾は、目標を達成するためにまだやるべきことが多く残っていることを明らかにしています。

IPv4 アドレス プールの制限を克服する取り組みにより、動的アドレス指定が使用されるようになりました。動的アドレス指定は、基本的に静的アドレス指定よりもはるかに複雑です。何らかの理由で、そのような制限がないにもかかわらず、動的メカニズムは IPv6 で使用され続けていますが、おそらく動的アドレス指定がプライバシーとセキュリティを保護するという一般的な素朴な信念のため、誰もその理論的根拠に疑問を抱いていないようです。実際には、これは初心者の侵入者の場合にのみ当てはまります。実際のところ、加害者は任意の被害者の具体的な身元を知る必要はありません。一方、学校、病院、企業、政府などの特定のエンティティをターゲットとする場合、その IP アドレスのほとんどは、問い合わせを容易にするために DNS（ドメイン ネーム システム）サービスを通じて簡単に入手できます。重大な犯罪者は、攻撃を開始するときに任意に変更できる架空のアドレスの背後に隠れることによってシステムの弱点を利用します。

さらに悪いことに、動的アドレスの慣行により、インターネットトラフィックの法医学的分析が非常に困難になり、犯罪防止を目的とした

法執行機関による無差別大量監視が正当化されてしまいました。他の当事者が同じことをするのを阻止するものは何もないので、もしそのように装備されていたとしても、最終的には、一般の個人にプライバシーは、たとえあったとしてもほとんど残されていません。これはかなり物議を醸し、複雑なトピックとなっています [3] 。

IPv4 の改良の代替として意図されていた IPv6 には下位互換性がないことが判明し、困難でコストのかかる移行となったことは大きな驚きでした。このため、暫定的なデュアルスタック プロトコル [4] の作成が必要になりましたが、コストは増加しましたが、元のハンディキャップはほとんど軽減されませんでした。

提案されているインターネット改善の最初の基準として、エンドツーエンドの接続が常に課されてきましたが、上記の課題の累積的な影響により、マスターを特徴とする CDN（コンテンツ配信ネットワーク – 現在主流のインターネット運用モデル）が誕生しました。スレーブ アーキテクチャは、たとえローカル コミュニティ内であっても、エンドユーザー間の直接的なピアツーピア通信を実際に妨げます。

インターネットの本来の価値提案のもう 1 つの部分は、公共通信システムを少数の大手電気通信プロバイダーによる独占や政府機関による規制から解放することでした。しかし、数十年が経ち、現在、インターネット サービスはいくつかのビジネス セクターに分割されており、それぞれのサービスを単一の有力な多国籍複合企業（およびいくつかの小規模な競合他社）が提供しています。このコングロマリットは非常に強力で影響力があるため、規制を回避しながら規制を回避することができます。それが生み出す問題。

同時に、日常的なインターネット運用への世界中の主権政府の関与が増大していることは、インターネットがスプリンターネットに細分化されることにつながるとして、多くの批判が寄せられています[5]。実際のところ、IAP（インターネット アクセス プロバイダー）はインターネット アーキテクチャを多くの AS（自律システム）[6] に分割しており、それらを相互接続するために BGP（ボーダー ゲートウェイ プロトコル）[7] を必要としています。地政学的なスプリンターネットは、単層の世界的通信ネットワークを各国の断片（合計約 195）[8] に分割することになりますが、AS はすでに球形ネットワークの層（現在約 76,000 個で増加中）[9] を作成しており、それぞれがそれらを包み込

んでいます。地球全体がタマネギの皮の完全な層のようになります。ある意味では、これらの「オニオンネット」層の数は、潜在的なスプリンターネットの断片の数よりも 2.5 桁近く多くなります。可能な AS の数が 32 ビット IPv4 アドレス プールと同じであることを認識する前でさえ、このコントラストは本当に驚くべきものです。 [10]。おそらく、スプリンターネットを批判することは、オニオンネットから注意をそらさせるための戦術です。

上記すべてを総合すると、インターネットの緊急事態の範囲を診断して理解するのに非常に多くの時間がかかることは驚くべきことではありません。悪意のあるハッキングの場合はさらに時間がかかり、数日、数週間、数か月、さらには場合によってはさらに時間がかかります。もっと長く – 大規模なサイバー攻撃の背後にいる当事者について推測を始めるだけです。比較すると、従来の PSTN（公衆交換電話網）では、通話に応答する前でも発信者の位置を特定できます。

要約すると、元の IPv4 ベースのインターネット設計では世界中のすべての人を明示的かつ一意に識別できないため、さまざまな動的な救済策が講じられました。残念なことに、これらの救済策は、正規ではあるが脆弱なユーザーを攻撃しようとする悪意のある加害者にとって完璧なカモフラージュにもなってしまいました。新しいバージョンの IPv6 には、すべての IoT（モノのインターネット）を識別するのに十分なアドレスがありますが、IPv4 の暫定スキームは引き続き存続します。さらに、IPv6 機能は、下位互換性がないためにデュアルスタック方式を使用せざるを得ず、純粋な IPv4 よりも複雑で高価であり、その結果、発展途上地域では IPv6 を採用することが困難になります。これらの複雑さにより、サイバー攻撃に対するネットワークの脆弱性が増大します。それにもかかわらず、インターネットのような継続的に使用される大規模システム、特にその全体を迅速に置き換えることは問題外です。

2. 要件:

この行き詰まりを回避するには、長期的なシステムに向けて進化しながら、現在の環境と共存できる現実的な解決策が必要です。理想的なアプローチは、進行中の運用を中断することなく、既存のシステムの一部のように動作するスキームを導入することですが、ベース施設と独立して機能するオーバーレイ ネットワークに進化する機能を備え、同時にベース施設間のアームズレングス インターフェイスを維持することです。相

互運用性と全体的なサービスの整合性のための 2 つです。これらは、同じテクノロジーを使用しながら、同等のサービスを提供するために異なる運用規律に従って並行して動作する 2 つのシステムに徐々に進化します。これにより、エンドユーザーは個人的に実験して両方の長所と短所を比較し、情報に基づいて望ましい長期的な構成を選択できるようになります。

3. 解決策:

幸いなことに、これまで議論された問題のほとんどに対処できるコンパクトなスキーム [11] が特定されました。このスキームの基本的なアプローチは、既存の CDN の構成要素である CG-NAT (キャリア グレード - ネットワーク アドレス変換) で長年予約されていた 240/4 ネットブロックを利用して、SPR (セミパブリック ルーター) と呼ばれる新しい機能を確立することです。現在のインターネット インフラストラクチャをオーバーレイします。このような展開のプロセスでは、長期にわたって新しいテクノロジーは必要ありません。

すべてのユーザーを識別するのに十分な静的アドレスがあるため、SPR には DHCP (動的ホスト構成プロトコル) が必要ないため、IAP に割り当てるアドレスが割り当てられなくなります。 DNS は本質的に電子電話と同等の準静的データベースに縮退するため、ホワイト ページと AS および BGP は不要になり、この新しいインターネット環境は大幅に簡素化されます。

長期間「予約」ステータスにあった 240/4 ネットブロックを使用するには、デバイスの機能をテストし、ネットワークのパフォーマンスを検証するためにすぐに利用できる機器を見つけるのが難しい場合があります。また、できるだけ多くの関係者がこの提案された移行を開始できるようにするために、そのような施設は簡潔、低コスト、学習曲線が最小限である必要があります。

以下に、実験とデモンストレーション用のテストベッドをセットアップするための基本的な機器とプロセスの概要を示します。後者から得たスキルと経験は、実際の SPR 導入を支援するために適用できます。

◦ 端末機器:

Xubuntu [12] V18.04.1 は、同じホストのノート PC (パーソナル コンピュータ) 上で同時に二重 IP アドレスを引き受けることが

できるため、最も便利な OS（オペレーティング システム）候補として特定されています。つまり、このような装備された各 PC は、同じハードウェア ネットワーク ポートを共有する 2 つの IoT、つまり、静的なクライアントと並んで共通の DHCP アドレス指定クライアントのように動作します。どちらも、使い慣れた IPv4 アドレスまたは 240/4 アドレスのいずれかを想定できます。このような PC 上の IPv4 DHCP IoT のペアは、従来のネットワーク プロセスを介してそれらの間の物理接続を確立できます。次に、同じ PC ペア上の静的な 240/4 アドレス指定された IoT は、240/4 環境での伝送特性を検証できます。この 2 段階のテストでは、ハードウェアのセットアップを変更したり、PC を再起動したりすることなく、メディアがいずれかのカテゴリの IPv4 アドレスを持つパケットを転送できる状態であることを確認します。さらに、これらの PC は、この媒体を通じて新しい IoT で使用され、現場に展開する前にその互換性を検証することができます。

- **ネットワークシミュレーター:**

240/4 互換テスト ベッドは、互換性のあるデバイスを認定し、その伝送パフォーマンスをチェックするための基本的なファブリックとして機能します。

A. 最終的な開始点として、商用 RG の長いリストをサポートする OpenWrt [13] ファームウェア V19.07.3 以降をインストールすることで、RG（ルーティング/住宅ゲートウェイ）を完全に 240/4 対応にする必要があります。これにより、従来の IoT と 240/4 アドレスを想定した IoT の両方にサービスを提供するオンプレミス LAN（ローカル エリア ネットワーク）と HAN（ホーム エリア ネットワーク）が確立され、インターネットに対して 240/4 DHCP クライアントのように動作します。

B. SPR として動作する構内（上記の RG で代表される）間に基本的な伝送ファブリックを提供するには、OpenWrt をサポートする D-Link スマート マネージド スイッチ DGS-1210 シリーズ [14] が適切な候補です。

SPR は構築中に、デフォルトのルーティング スキームが階層化されることを除いて、既存の CG-NAT ファブリックと同じ機能を備えた同じ施設に本質的にサービスを提供するオーバーレイ ネットワークを形

成します。このプロセスを複製して、最終的に CG-NAT クラスター全体をオーバーレイすることができます。次に、100.64/10 ネットブロックの 64 倍である 240/4 ネットブロック サイズを最大限に活用することで、1 つの SPR から複数の CG-NAT クラスターにサービスを提供できます。これにより、CG-NAT クラスターの容量に制限が設定されます。動的再割り当て。サービスを受ける人口の規模に応じて、RAN（地域エリアネットワーク）[15] は 1 つまたは複数の SPR で構成される場合があります。

4. 結論:

240/4 ネットブロックは長年にわたり「将来の使用のために予約済み」または「実験用」として正式に指定されてきたため、使用できるかどうかについての疑問が当然生じました。多国籍企業複合体が、発表なしにさまざまな目的で 240/4 ネットブロックを実際に使用していると報告されています [16]。このようなアクティビティを発見するのにある程度の労力がかかったという事実は、240/4 ネットブロックの使用によって既存のインターネットの運用が中断されず、今後も中断されないことを示しています。したがって、240/4 ネットブロックは、提案されている SPR を展開するための理想的な手段です。

静的アドレスを使用することで、RAN は階層型ルーティングを介してインターネット操作を合理化し、多国籍企業による支配から解放され、一般の人々がピアツーピア通信を楽しめるようになります。既存の CDN ベースのインターネットよりも決定的であるため、サイバー侵入に対してより堅牢です。

詳細については、この提案をよりビジネス指向の観点から分析したオンライン ホワイトペーパー [17] を参照してください。

参考文献:

[1] 人口別の世界の国。
https://www.worldometers.info/world-population/population-by-country/

[2] IPv4 アドレス割り当て別の国一覧:
https://en.wikipedia.org/wiki/List_of_countries_by_IPv4_address_allocation

[3] サイバーセキュリティ脆弱性状況
https://blog.apnic.net/2021/02/03/the-internet-of-trash/

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

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

[6] 自律システム
https://en.wikipedia.org/wiki/Autonomous_system_(Internet)

[7] ボーダーゲートウェイプロトコル
https://en.wikipedia.org/wiki/Border_Gateway_Protocol

[8] 世界の国
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] 現在の AS の数
https://thyme.apnic.net/current/data-summary

[10] 自律システム番号
https://www.arin.net/resources/guide/asn/

[11] 米国特許第 11,159,425 号
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 シリーズ スマート スイッチ
https://www.dlink.com/us/en/products/dgs-1210-series-gigabit-smart-plus-switches

[15] リージョナルエリアネットワークシミュレータ
https://www.avinta.com/gallery/RegionalAreaNetworkSimulator.pdf

[16] 240/4 の未発表の使用
https://labs.ripe.net/author/qasim-lone/2404-as-seen-by-ripe-atlas/

[17] インターネットを刷新する:
https://www.avinta.com/gallery/RevampTheInternet.pdf

用語、略語、頭字語:

. AS: 自律システム

. BGP: ボーダー ゲートウェイ プロトコル

. CDN: コンテンツ配信ネットワーク

. CG-NAT: キャリアグレードのネットワークアドレス変換

. DHCP: 動的ホスト構成プロトコル

. DNS: ドメイン ネーム システム

. Dual-Stack: IPv4 アドレスと IPv6 アドレスの両方の同時使用をサポートするネットワーク環境。

. HAN: ホーム エリア ネットワーク (個人/住宅関係者向けのオンプレミス ネットワーク)

. IAP: インターネット アクセス プロバイダー

. IoT: モノのインターネット

. IPv4: インターネット プロトコル バージョン 4

. IPv6: インターネット プロトコル バージョン 6

. LAN：ローカルエリアネットワーク（機関が利用するオンプレミスネットワーク）

. OS: オペレーティング システム

.PC：パーソナルコンピュータ

. PSTN: 公衆交換電話網

. RAN: リージョナル エリア ネットワーク

. RG: ルーティング/住宅用ゲートウェイ

. SPR: 準パブリックルーター

. 240/4 ネットブロック: 240.0.0.0 から 255.255.255.255 までの IPv4 アドレス プール。およそ 2 億 5,600 万 (2 億 5,600 万) または 25 億の 4 分の 1 (0.2 億 5,600 万) のアドレスに相当します。は「実験用」または「将来の使用」のために「予約済み」に指定されました。

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