# 簡化網際網路

## 1. 背景：

網際網路的快速採用與廣泛部署，使其成為事實上的全球通訊骨幹，但同時也產生了各種嚴重的問題，從網路騷擾、安全漏洞到贖金軟體，不一而足。其中許多問題的根源可追溯至 IPv4 位址池短缺。

長久以來，人人享有公平競爭的環境一直是網際網路價值主張的重要部分。然而，即使在基本的位址分配實務中，這也不是現實。根據世界人口[1]和目前的 IPv4 分配[2]，美國人均擁有 4.91 個位址，而尚比亞只佔 0.01 個，比例超過兩個半級數。梵蒂岡市人均擁有 21.44 個位址，而世界上有十多個國家卻一個位址也沒有。這些鮮明的差異說明，要達到目標仍有許多工作要做。

克服 IPv4 位址池限制的努力導致動態位址的使用，而動態位址從根本來說比靜態位址要複雜得多。由於某些原因，動態機制在沒有這些限制的情況下仍被用於 IPv6，而且似乎沒有人質疑其合理性，這也許是因為人們普遍天真的認為動態位址可以保護隱私和安全。事實上，只有新手入侵者才會相信這一點。事實上，犯罪者不需要知道任意受害者的特定識別資訊。另一方面，當以特定實體 (例如學校、醫院、企業、政府等) 為目標時，他們大部分的 IP 位址都可以隨時透過 DNS (網域名稱系統) 服務查詢。嚴重的犯罪者會利用系統的弱點，躲在虛構的位址後面，而這些位址在他們發動攻擊時可以任意變更。

更糟的是，動態位址的做法使得網際網路流量的鑑識分析變得如此困難，以至於執法單位為了預防犯罪而不分青红皂白地進行大規模監控變得合情合理。由於沒有任何東西可以阻止任何其他方做同樣的事情，如果有這樣的設備的話，歸根結柢，普通個

人的隱私就所剩無幾了！這已成為一個頗具爭議且複雜的議題 [3] 。

IPv6 原本是用來取代 IPv4 的，但令人大吃一驚的是，IPv6 竟然無法向下相容，這使得過渡過程充滿挑戰且成本高昂。因此有必要建立臨時的雙堆疊通訊協定 (Dual-Stack Protocol) [4]，在增加成本的同時，也無法真正紓緩原本的障礙。

端對端的連線性一直是任何網際網路改進提案的首要標準，但上述挑戰的累積效果已導致 CDN（內容傳輸網路 - 目前最主要的網際網路運作模式），其特點是主從式架構，實際上妨礙了終端使用者之間直接的點對點通訊，即使是在本地社區內也是如此。

網際網路最初價值主張的另一個部分，是讓公共通訊系統不再被幾家大型電信業者壟斷，也不再受到政府機關的管制。然而，數十年後的今天，網際網路服務已被分割為數個商業領域，每個領域都由單一的主導性跨國企業集團 (以及幾個較小的競爭者) 提供服務。它是如此強大和有影響力，以至於它能夠逃避法規，同時淡化它所造成問題的責任。

與此同時，許多人批評全球主權政府日益參與網際網路的日常運作，導致網際網路分裂成一個 Splinternet [5]。事實上，IAPs（網際網路存取供應商）已經將網際網路架構分割成許多 ASes（自治系統）[6]，需要 BGP（邊界閘道協定）[7]來互連。地緣政治的 Splinternet 會將單層的全球通訊網路分割成各個國家的片段（總數約為 195 個）[8]，而 ASes 已經建立了各層（目前約有 76K 個，而且還在增加中）[9] 的球形網路，每個球形網路都像一層完整的洋蔥皮一樣包覆著整個地球。從某種意義上說，這些「洋蔥網」層數比潛在的 Splinternet 片段多出近兩個半階級。這種對比確實令人匪夷所思，即使還沒意識到可能的 AS 數量與 32 位元

IPv4 位址池相同！[10]. 也許批評 Splinternet 是一種策略，目的是要轉移人們對洋蔥網的注意力。

綜合以上所述，不難發現診斷和瞭解緊急網際網路事件的程度需要如此長的時間，而在惡意駭客攻擊的情況下，更需要數天、數週、數月甚至更長的時間，才能剛開始推測重大網路攻擊的幕後主腦。相較之下，傳統的 PSTN (公共交換電話網路) 甚至在電話接聽之前就能定位來電者。

總而言之，由於基於 IPv4 的原始網際網路設計無法明確且唯一地識別世界上的每個人，因此產生了各種動態的補救方法。不幸的是，這些補救方法也為惡意的犯罪者提供了完美的偽裝，他們意圖攻擊合法但易受攻擊的使用者。雖然新版 IPv6 的位址足以識別所有 IoT（物聯網），但 IPv4 的臨時方案仍在繼續延續。此外，IPv6 設施因缺乏向後相容性而被迫使用 Dual-Stack 方案，比純 IPv4 更為複雜且昂貴，結果是發展中地區很難採用 IPv6。這些複雜性增加了網路遭受網路攻擊的脆弱性。儘管如此，要快速取代任何像網際網路這樣持續使用的大型系統，尤其是整個系統，是不可能的事。

## 2. 要求：

為了擺脫這種僵局，實際的解決方案必須能夠與目前的環境共存，同時朝向長期系統演進。理想的方法是引入一個方案，其行為就像現有系統的一部分 - 不會中斷正在進行的作業 - 但有能力演進為一個獨立於基礎設施運作的覆蓋網路，同時維持兩者之間的等距介面，以達到互通性和整體服務完整性。這將逐漸演進為兩個平行運作的系統，使用相同的技術，但遵循不同的作業規範，以提供相若的服務。這將賦予終端使用者親自嘗試和比較兩者利弊的能力，以便對首選的長期配置做出明智的選擇。

## 3. 解決方案：

幸運的是，我們找到了一個精簡的方案 [11]，可以處理目前討論的大部分問題。此方案的基本方法是利用現有 CDN 建置區塊 CG-NAT (Carrier Grade - Network Address Translation) 中長期保留的 240/4 網路區塊，建立稱為 SPR (Semi-Public Router) 的新設施，以覆蓋目前的網際網路基礎架構。在長時間部署的過程中，不需要任何新技術。

有了足夠的靜態位址來識別每個使用者，SPR 就不需要 DHCP (動態主機設定通訊協定)，這使得 IAP 無法分配位址。DNS 基本上淪為等同於電子電話白頁的準靜態資料庫，AS 和 BGP 也不再需要，因此新的網際網路環境簡化許多。

要使用長期處於「保留」狀態的 240/4 網塊，可能很難找到現成的設備來測試裝置能力及驗證網路效能。此外，這樣的設備必須簡潔、成本低、學習曲線最小，以鼓勵盡可能多的有興趣者啟動這項建議的過渡。

以下概述了建立實驗和示範測試台的基本設備和流程。從後者獲得的技能和經驗可以用來協助實際的 SPR 部署。

### . 終端儀器：

Xubuntu [12] V18.04.1 被認為是最方便的 OS（作業系統），因為它可以在同一台筆記型電腦（個人電腦）主機上同時使用雙 IP 位址。也就是說，每台這樣配備的 PC 就像是共用相同硬體網路連接埠的兩個 IoT，即一個共用 DHCP 位址的用戶端和一個靜態用戶端。兩者都可以使用熟悉的 IPv4 或 240/4 位址。這類 PC 上的一對 IPv4 DHCP IoT 可透過傳統的網路程序建立彼此間的實體連線。之後，同一對 PC 上的靜態 240/4 位址 IoT 就可以驗證

240/4 環境中的傳輸特性。在不變更任何硬體設定或重新啟動 PC 的情況下，這兩個步驟的測試可確保媒體已準備好傳輸任何 IPv4 位址的封包。此外，在部署到現場之前，這些 PC 可以透過此媒介與新的 IoT 一起使用，以驗證其相容性。

- **網路模擬器：**

240/4 相容的測試平台可作為驗證相容裝置和檢查其傳輸效能的基本結構。

A. 為了一個明確的起點，應安裝 OpenWrt [13] 韌體 V19.07.3 或更高版本，使 RG (路由/住宅閘道器) 完全支援 240/4，此韌體支援一長串的商用 RG。這將會建立企業內部的 LAN (區域網路) 和 HAN (家庭區域網路)，可同時為傳統的 IoT 和假設 240/4 位址的 IoT 提供服務，同時表現得像網際網路的 240/4 DHCP 客戶端。

B. 為了在以 SPR 運作的處所（以上述 RG 為代表）之間提供基本的傳輸結構，支援 OpenWrt 的 D-Link 智慧型管理交換器 DGS-1210 系列 [14] 是很好的選擇。

當 SPR 正在建立時，它會形成一個覆蓋網路，除了預設路由方案變為分層之外，該覆蓋網路基本上服務於與現有 CG-NAT 架構具有相同功能的相同處所。這個過程可以複製，最終覆蓋整個 CG-NAT 集群。接下來，透過充分利用 240/4 網塊大小（為 100.64/10 網塊的 64 倍），可從單一 SPR 為多個 CG-NAT 群組提供服務，該網塊設定了 CG-NAT 群組在無動態重新分配情況下的容量限制。區域網路 (Regional Area Network) [15] 可由一個或多個 SPR 組成，視服務人口的大小而定。

## 4. 結論：

由於 240/4 網區多年來一直被正式指定為「保留給未來使用」或「實驗性」，因此自然會產生是否可以使用的疑問。據報

導，跨國企業集團在沒有公告的情況下，實際上已將 240/4 網區用於各種用途 [16]。花了一些功夫才發現這些活動的事實顯示，240/4 網區的使用並沒有、也不會擾亂現有的網際網路作業。因此，240/4 網區是部署所建議的 SPR 的理想工具。

使用靜態位址，RAN 將可透過分層路由方式簡化網際網路運作，讓一般大眾享有點對點通訊，不受跨國企業集團的支配。定址方案的靜態性質使 RAN 比現有以 CDN 為基礎的網際網路更具決定性，因此更能抵擋網路入侵。

如需詳細資訊，有一份線上白皮書 [17]，從更商業導向的角度分析這項提案。

## 參考資料：


[1] 世界各國人口；
https://www.worldometers.info/world-population/population-by-country/

[2] 按 IPv4 位址分配的國家清單：
https://en.wikipedia.org/wiki/List_of_countries_by_IPv4_address_allocation

[3] 網路安全弱點狀況
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(also%20referred%20to,religion%2C%20and%20divergent%20national%20interests.

[6] 自治系統
https://en.wikipedia.org/wiki/Autonomous_system_(Internet)

[7] 邊界閘道通訊協定
https://en.wikipedia.org/wiki/Border_Gateway_Protocol

[8] 世界各國
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] 目前 AS 的數目
https://thyme.apnic.net/current/data-summary

[10] 自治系統號碼
https://www.arin.net/resources/guide/asn/

[11] 美國專利編號 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 系列智慧型交換器
https://www.dlink.com/us/en/products/dgs-1210-series-gigabit-smart-plus-switches

[15] 區域網路模擬器
https://www.avinta.com/gallery/RegionalAreaNetworkSimulator.pdf

[16] 使用 240/4 未通知
https://labs.ripe.net/author/qasim-lone/2404-as-seen-by-ripe-atlas/

[17] 改造網際網路：
https://www.avinta.com/gallery/RevampTheInternet.pdf

**術語、縮寫和首字母縮寫：**

. AS：自治系統

. BGP：邊界閘道協定

. CDN： 內容傳送網路 .

. CG-NAT： 電信級網路位址轉換

. DHCP： 動態主機組態協定

. DNS：網域名稱系統

. Dual-Stack：雙堆疊： 支援同時使用 IPv4 和 IPv6 位址的網路環境

. HAN：家庭區域網路 (Home Area Network)（私人/住宅單位的內部網路）

. IAP： 網際網路存取供應商

. IoT：物聯網

. IPv4：網際網路協定版本 4

. IPv6：網際網路協定版本 6

. LAN：區域網路（機構使用的內部網路）

. OS：作業系統

. PC：個人電腦

. PSTN： 公共交換電話網路

. RAN：區域網路

. RG：路由/住宅閘道

. SPR: 半公共路由器

. 240/4 Netblock： 範圍從 240.0.0.0 到 255.255.255.255 的 IPv4 位址池，總數約為 2.56 億 (256M) 或四分之一億 (0.256B)，自 1981-09 年以來一直未正式使用，因為這些位址被指定為「實驗性」或「保留」給「未來使用」。

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