網路安全神話

介紹

儘管互聯網在過去幾十年中取得了驚人的發展，但至今仍然脆弱不堪，容易受到各種規模的攻擊。使用者對網路複雜的運作機制感到困惑，往往無法區分是駭客入侵還是防護軟體本身出現了故障。

最近發生的類似事件是在 2025 年 11 月 18 日，當時 Cloudflare 遭遇了全球性故障，導致網路大面積癱瘓了一段時間[1]。這並非個案。上一次故障發生在僅僅八個月前，在此之前也發生過多次類似事件。同樣，亞馬遜網路服務 (AWS) 也頻繁出現故障[2]。這種網路中斷幾乎已成為常態，人們開始質疑這些旨在抵禦網路入侵的服務是否可靠。

問題

網路的脆弱性問題已經存在了幾十年。去年，美國聯邦通訊委員會（FCC）發布了一份擬議規則制定通知（NPRM）[3]，其中指出邊界網關協定（BGP）[4] 是降低風險的關鍵目標。代表互聯網社區的互聯網架構委員會（IAB）對此發表評論，表達了擔憂 [5]。儘管如此，白宮還是發布了一份路線圖 [6]，重點在於 BGP 的完整性，以增強網路路由的安全性。

在這方面，重要的是要記住，BGP 協定負責在自治系統（AS）[7] 之間傳輸資料包，這些自治系統由網域名稱伺服器（DNS）[8] 根據動態主機配置協定（DHCP）[9] 分配給使用者的 IPv4 位址進行選擇。而 DHCP 協定最初是為了解決 IPv4 位址短缺問題而創建的。這種協定棧導致了複雜的系統架構，容易受到來自多個方面的攻擊，每一種攻擊都需要相應的修補程式來應對。

解決方案

一個有缺陷的系統會導致一系列永無止境的修補和改進。而一個簡化且精簡的架構可以建構一個更健壯的互聯網，徹底消除 IPv4 位址短缺的根本原因，因此無需使用上述四種協定。這正是名為 EzIP[10] 的確定性系統所帶來的成果。

技術和架構演進

當網路最初出現時，明確定義的大型 IPv4 位址區塊被分配給了五個區域網路註冊機構 (RIR)。例如，希爾伯特曲線 [11] 圖中清楚顯示了早期 AFRINIC（非洲）、APNIC（亞太地區）、ARIN（北美）、LACNIC（拉丁美洲和加勒比地區）和 RIPE（歐洲、中東和中亞）的分配情況 [12]。

儘管每個區域網路註冊機構 (RIR) 將其分配到的位址分配給其所在區域的網路存取供應商 (IAP)，但 IAP 本身並不需要遵守相同的限制。這導致了 IP 位址碎片化問題的出現，使得使用者的實際地理位置與其分配到的 IP 位址最初分配的區域不再具有地理關聯性。

隨著 IPv4 位址池逐漸枯竭，DHCP 透過動態重複使用可用的公共 IPv4 位址來維持網際網路存取服務（IAP）的運作。隨後引入了 DNS，以減輕這種不斷變化的環境對用戶的負擔。由於這對協定組合似乎能夠滿足當時的迫切需求，因此它成為了預設的網路建構模組。（請參閱註腳以了解這種特殊組合帶來的影響。）

由於早期採用IPv4的機構同意將剩餘的IPv4位址區塊公開拍賣，以緩解IPv4位址池枯竭的壓力，因此，期望IPv4位址包含任何有意義的實體位置資訊已不再現實，更不用說透過IPv4位址對用戶進行地理位置定位了。為了滿足這項需求，一個新的產業分支應運而生。然而，其報告的分辨率和準確性往往令人質疑 [13]。

在此過程中，擁有一個或多個 IPv4 位址區塊的網際網路存取供應商 (IAP) 開發了各自的 IP 封包傳輸方案。共享相同傳輸策略的位址區塊被分組在一起，形成一個自治系統 (AS)。由於每個 AS 的範圍各不相同且通常有限，因此需要依靠 BGP 協定來跨越 AS 邊界轉送 IP 封包。隨著 AS 數量的增長，負責資料包傳輸的 BGP 協定的複雜性也隨之增加，尤其對於那些需要傳輸較遠距離（通常僅限於本地）的資料包，更不用說那些需要跨越多個 AS 邊界才能到達全球位址的資料包了。

儘管這些協議本質上都是分散式的，但它們的操作確實需要大量的協調，而這種協調依賴於中心化的機制，從而導致少數資源豐富的企業佔據主導地位，例如內部分發網路（CDN）[14] 運營商，包括 Cloudflare、AWS 等。這些企業成為了網路傳輸設施的核心基礎設施。

矛盾

網路上有許多做法，使得其原理和運作方式令人費解：

網路促進了公平競爭。但梵蒂岡城人均獲得 21.4 個 IPv4 位址分配，而十幾個實體卻一個都沒有，其他國家的分配數量則介於兩者之間[15]。（註：塞席爾人均獲得 58.4 個地址分配是一個特例，這是由於企業利用當地政治環境尋求全球商機所致。）

互聯網最初承諾實現端到端連接。然而，目前其主流運作模式—內容分發網路（CDN）—即使在本地社群內，也阻礙了這一目標的實現。

網路最初的出現是為了挑戰電信公司的壟斷地位和政府對公共交換電話網路（PSTN）的監管。然而，如今網路卻被跨國企業集團所主導，這些企業幾乎壟斷了各自的業務領域，甚至到了漠視責任、逃避監管的地步。這種中心化不正是與網路最初的分散式願景背道而馳嗎？

此外，大約 200 個全球司法管轄區可能導致網路分裂，形成地緣政治上的「分裂互聯網」（Splinternet）[16]，這種可能性正受到網路界的批評。同時，自治系統（AS）已經使網路變成了一個擁有至少 7.7 萬個層級的「洋蔥網路」[7]。更糟的是，由於大多數自治系統只選擇性地為世界部分地區提供服務，因此洋蔥網路的每一層都更像是一張佈滿漏洞的殘缺漁網！

最令人費解的是，網路極力維護其無國界原則，而其主要的路由機制卻演變成了 BGP，其中的「B」恰恰代表著每個自治系統（AS）的邊界！

總的來說，由於這些協定具有高度複雜、動態和分散的特性，網路很容易受到各種惡意安全攻擊，從日常騷擾到勒索軟體攻擊，無所不包。

或許此時有必要指出，IPv6 在沒有充分利用自身龐大位址池的情況下，竟然沿用了這些源自於臨時需求的 IPv4 實踐。如今，IPv6 的重要性似乎正在悄悄消退[17]，而人們也不再提及 IPv4 的淘汰日期。由於 IPv6 相對於 IPv4 並沒有展現出任何顯著優勢，大多數正在進行的網路討論也不再區分兩者。

參考

1. Cloudflare 服務中斷歷史記錄 (2019-2025)
   https://controld.com/blothe/biggest-cloudflare-outages/

2. AWS 雲端服務與資料中心故障歷史記錄：
   https://www.datacenterknowledge.com/outages/a-history-of-aws-cloud-and-data-center-outages

3. 關於邊界網關協定風險緩解進展的報告；安全互聯網路由
   https://www.federalregister.gov/documents/2024/06/17/2024-13048/reporting-on-border-gateway-protocol-risk-mitigation-progress-secure-internet-routing

4. 邊界網關協議
   https://en.wikipedia.org/wiki/Border_Gateway_Protocol

5. 互聯網協會、互聯網架構委員會和互聯網名稱與數位地址分配機構就「關於邊界網關協議風險緩解進展的報告」一事發表的評論"
   https://datatracker.ietf.org/doc/statement-iab-comments-of-the-internet-society-internet-architecture-board-and-internet-corporation-for-assigned-names-and-numbers-in-the-matter-of-reporting-on-border-gateway-protocol-risk-mitigation-progress/

6. 增強網際網路路由安全性的路線圖
   https://bidenwhitehouse.archives.gov/wp-content/uploads/2024/09/Roadmap-to-Enhancing-Internet-Routing-Security.pdf

7. 自治系統（網際網路）
   https://en.wikipedia.org/wiki/Autonomous_system_(Internet)

8. 域名系統
   https://en.wikipedia.org/wiki/Domain_Name_System

9. 動態主機配置協定
   https://en.wikipedia.org/wiki/Dynamic_Host_Configuration_Protocol

10. 確定性互聯網
    https://avinta.com/gallery/DeterministicInternet-SPKR.pdf

11. 希爾伯特曲線

https://en.wikipedia.org/wiki/Hilbert_curve

12. 使用希爾伯特曲線可視化 IPv4 位址空間
    https://thebayesianobserver.wordpress.com/2011/10/23/121/

13. 網路地理位置
    https://en.wikipedia.org/wiki/Internet_geolocation

14. 內容傳遞網絡
    https://en.wikipedia.org/wiki/Content_delivery_network

15. 按 IPv4 位址分配情況列出的國家列表
    https://en.wikipedia.org/wiki/List_of_countries_by_IPv4_address_allocation

16. 分裂網路
    https://en.wikipedia.org/wiki/Splinternet

17. 傑夫赫斯頓：網路的過去、現在與未來
    (TM: 1:08:18, “IPv6—越來越無關緊要”)
    https://cloudflare.tv/this-week-in-net/geoff-huston-the-internet-s-past-present-and-future/dg78lmvO

註腳

DHCP 和 DNS 是多年來一直困擾著所有人的最令人費解的網路技術組合。DHCP 透過根據需要動態分配 IP 位址來保障使用者的個人隱私，但這種隱私保護卻立即被 DNS 徹底否定，因為 DNS 會根據請求方的身份，提供該方最新分配到的 IP 位址！這使得一般使用者像鴕鳥一樣，誤以為自己受到了保護，而同時，大量的 IT 工程師卻因此獲得了穩定的工作。這完美地詮釋了中國成語「矛與盾」的涵義。

然而，基於這種方案，人們在自治系統（AS）和邊界網關協議（BGP）的基礎上不斷構建更多層級的協議，最終形成了內容分發網路（CDN），從而鞏固了跨國公司的統治地位，並催生了諸如 Cloudflare 和 AWS 等大型服務商，它們承諾提供更安全可靠的資料傳輸服務。然而，這些服務的可靠性卻屢屢受到質疑。當網路遭受攻擊時，似乎沒有人願意承擔責任，也沒有人願意尋找其他方案來降低漏洞風險。或許是因為整個網路如此分散，所以很難追究責任？

另一方面，目前的網路配置為攻擊者提供了理想的便利條件。攻擊者可以隨意偽造任何虛假的 IP 位址，冒充合法的普通網路使用者發動攻擊，然後在攻擊結束後放棄該位址，幾乎不留下任何帶有真實身分資訊的永久記錄，從而難以進行取證追蹤。