网络安全神话

介绍

尽管互联网在过去几十年取得了惊人的发展，但至今仍然脆弱不堪，容易受到各种规模的攻击。用户对互联网复杂的运作机制感到困惑，往往无法区分是黑客入侵还是防护软件本身出现了故障。

最近发生的一起类似事件是在 2025 年 11 月 18 日，当时 Cloudflare 遭遇了全球性故障，导致互联网大面积瘫痪了一段时间[1]。这并非孤立事件。上一次故障发生在仅仅八个月前，而在此之前也发生过多次类似事件。同样，亚马逊网络服务 (AWS) 也频繁出现故障[2]。这种互联网中断几乎已成为常态，人们开始质疑这些旨在抵御网络入侵的服务是否可靠。

问题

互联网的脆弱性问题已经存在了几十年。去年，美国联邦通信委员会（FCC）发布了一份拟议规则制定通知（NPRM）[3]，其中指出边界网关协议（BGP）[4] 是降低风险的关键目标。代表互联网社区的互联网架构委员会（IAB）对此发表评论，表达了担忧 [5]。尽管如此，白宫还是发布了一份路线图 [6]，重点关注 BGP 的完整性，以此增强互联网路由的安全性。

在这方面，重要的是要记住，BGP 协议负责在自治系统（AS）[7] 之间传输数据包，这些自治系统由域名服务器（DNS）[8] 根据动态主机配置协议（DHCP）[9] 分配给用户的 IPv4 地址进行选择。而 DHCP 协议最初是为了解决 IPv4 地址短缺问题而创建的。这种协议栈导致了复杂的系统架构，容易受到来自多个方面的攻击，每一种攻击都需要相应的补丁来应对。

解决方案

一个存在缺陷的系统会导致一系列永无止境的修补和改进。而一个简化且精简的架构可以构建一个更加健壮的互联网，彻底消除 IPv4 地址短缺的根本原因，从而无需使用上述四种协议。这正是名为 EzIP[10] 的确定性系统所带的成果。

技术和架构演进

互联网最初出现时，明确定义的大型 IPv4 地址块被分配给了五个区域互联网注册机构 (RIR)。例如，希尔伯特曲线 [11] 图中清晰地显示了早期 AFRINIC（非洲）、APNIC（亚太地区）、ARIN（北美）、LACNIC（拉丁美洲和加勒比地区）和 RIPE（欧洲、中东和中亚）的分配情况 [12]。

尽管每个区域互联网注册机构 (RIR) 将其分配到的地址分配给其所在区域的互联网接入提供商 (IAP)，但 IAP 本身并不需要遵守同样的限制。这导致了 IP 地址碎片化问题的出现，使得用户的实际地理位置与其分配到的 IP 地址最初分配的区域不再具有地理关联性。

随着 IPv4 地址池逐渐枯竭，DHCP 通过动态重用可用的公共 IPv4 地址来维持互联网接入服务（IAP）的运行。随后引入了 DNS，以减轻这种不断变化的环境给用户带来的负担。由于这对协议组合似乎能够满足当时的迫切需求，因此它成为了默认的互联网构建模块。（参见脚注了解这种特殊组合带来的影响。）

由于早期采用 IPv4 的机构同意将剩余的 IPv4 地址块公开拍卖，以缓解 IPv4 地址池枯竭的压力，因此，期望 IPv4 地址包含任何有意义的物理位置信息已不再现实，更不用说通过 IPv4 地址对用户进行地理位置定位了。为了满足这一需求，一个新的行业分支应运而生。然而，其报告的分辨率和准确性往往令人质疑 [13]。

在此过程中，拥有一个或多个 IPv4 地址块的互联网接入提供商 (IAP) 开发了各自的 IP 数据包传输方案。共享相同传输策略的地址块被分组在一起，形成一个自治系统 (AS)。由于每个 AS 的范围各不相同且通常有限，因此需要依靠 BGP 协议来跨越 AS 边界转发 IP 数据包。随着 AS 数量的增长，负责数据包传输的 BGP 协议的复杂性也随之增加，尤其对于那些需要传输较远距离（通常仅限于本地）的数据包，更不用说那些需要跨越多个 AS 边界才能到达全球地址的数据包了。

尽管这些协议本质上都是分布式的，但它们的操作确实需要大量的协调，而这种协调依赖于中心化的机制，从而导致少数资源丰富的企业占据主导地位，例如内容分发网络（CDN）[14] 运营商，包括 Cloudflare、AWS 等。这些企业成为了互联网传输设施的核心基础设施。

矛盾

互联网上存在许多做法，使得其原理和运作方式令人费解：

互联网促进了公平竞争。但梵蒂冈城人均获得 21.4 个 IPv4 地址分配，而十几个实体却一个都没有，其他国家/地区的分配数量则介于两者之间[15]。（注：塞舌尔人均获得 58.4 个地址分配是一个特例，这是由于企业利用当地政治环境寻求全球商机所致。）

互联网最初承诺实现端到端连接。然而，目前其主流运行模式—内容分发网络（CDN）—即使在本地社区内，也阻碍了这一目标的实现。

互联网最初的出现是为了挑战电信公司的垄断地位和政府对公共交换电话网络（PSTN）的监管。然而，如今互联网却被跨国企业集团所主导，这些企业几乎垄断了各自的业务领域，甚至到了漠视责任、逃避监管的地步。这种中心化难道不正是与互联网最初的分布式愿景背道而驰吗？

此外，大约 200 个全球司法管辖区可能导致互联网分裂，形成地缘政治上的“分裂互联网”[16]，这种可能性正受到互联网界的批评。与此同时，自治系统（AS）已经使互联网变成了一个拥有至少 7.7 万个层级的“洋葱网络”[7]。更糟糕的是，由于大多数自治系统只选择性地为世界部分地区提供服务，因此洋葱网络的每一层都更像是一张布满漏洞的残缺渔网！

最令人费解的是，互联网极力维护其无国界原则，而其主要的路由机制却演变成了 BGP，其中的“B”恰恰代表着每个自治系统（AS）的边界！

总的来说，由于这些协议具有高度复杂、动态和分布式的特性，互联网很容易受到各种恶意安全攻击，从日常骚扰到勒索软件攻击，无所不包。

或许此时有必要指出，IPv6 在没有充分利用自身庞大地址池的情况下，竟然沿用了这些源于临时需求的 IPv4 实践。如今，IPv6 的重要性似乎正在悄然消退[17]，而人们也不再提及 IPv4 的淘汰日期。由于 IPv6 相对于 IPv4 并没有展现出任何显著优势，大多数正在进行的互联网讨论也不再区分两者。

参考

1. Cloudflare 服务中断历史记录 (2019-2025)
   https://controld.com/blothe/biggest-cloudflare-outages/

2. AWS 云服务和数据中心故障历史记录
   https://www.datacenterknowledge.com/outages/a-history-of-aws-cloud-and-data-center-outages

3. 关于边界网关协议风险缓解进展的报告；安全互联网路由
   https://www.federalregister.gov/documents/2024/06/17/2024-13048/reporting-on-border-gateway-protocol-risk-mitigation-progress-secure-internet-routing

4. 边界网关协议
   https://en.wikipedia.org/wiki/Border_Gateway_Protocol

5. 互联网协会、互联网架构委员会和互联网名称与数字地址分配机构就“关于边界网关协议风险缓解进展的报告”一事发表的评论
   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. 增强互联网路由安全性的路线图
   https://bidenwhitehouse.archives.gov/wp-content/uploads/2024/09/Roadmap-to-Enhancing-Internet-Routing-Security.pdf

7. 自治系统（互联网）
   https://en.wikipedia.org/wiki/Autonomous_system_(Internet)

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

9. 动态主机配置协议
   https://en.wikipedia.org/wiki/Dynamic_Host_Configuration_Protocol

10. 确定性互联网
    https://avinta.com/gallery/DeterministicInternet-SPKR.pdf

11. 希尔伯特曲线

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

12. 使用希尔伯特曲线可视化 IPv4 地址空间
    https://thebayesianobserver.wordpress.com/2011/10/23/121/

13. 互联网地理位置
    https://en.wikipedia.org/wiki/Internet_geolocation

14. 内容分发网络
    https://en.wikipedia.org/wiki/Content_delivery_network

15. 按 IPv4 地址分配情况列出的国家/地区列表
    https://en.wikipedia.org/wiki/List_of_countries_by_IPv4_address_allocation

16. 分裂互联网
    https://en.wikipedia.org/wiki/Splinternet

17. 杰夫·赫斯顿：互联网的过去、现在和未来
    (TM: 1:08:18, “IPv6——越来越无关紧要”)
    https://cloudflare.tv/this-week-in-net/geoff-huston-the-internet-s-past-present-and-future/dg78lmvO

脚注

DHCP 和 DNS 是多年来一直困扰着所有人的最令人费解的互联网技术组合。DHCP 通过根据需要动态分配 IP 地址来保障用户的个人隐私，但这种隐私保护却立即被 DNS 彻底否定，因为 DNS 会根据请求方的身份，提供该方最新分配到的 IP 地址！这使得普通用户像鸵鸟一样，误以为自己受到了保护，而与此同时，大量的 IT 工程师却因此获得了稳定的工作。这完美地诠释了中国成语“矛与盾”的含义。

然而，基于这种方案，人们在自治系统（AS）和边界网关协议（BGP）的基础上不断构建起更多层级的协议，最终形成了内容分发网络（CDN），从而巩固了跨国公司的统治地位，并催生了诸如 Cloudflare 和 AWS 等大型服务商，它们承诺提供更安全可靠的数据传输服务。然而，这些服务的可靠性却屡屡受到质疑。当互联网遭受攻击时，似乎没有人愿意承担责任，也没有人愿意寻找其他方案来降低漏洞风险。或许是因为整个互联网如此分散，所以很难追究责任？

另一方面，目前的互联网架构为攻击者提供了便利，他们可以随意伪造任何虚假的 IP 地址，冒充合法的普通互联网用户发起攻击，之后又迅速放弃该地址，几乎不留下任何带有真实身份信息的永久记录，从而难以进行取证追踪。

.