精简互联网

1. 背景：

互联网被迅速采用并广泛部署，成为事实上的全球通信骨干网，与此同时，也出现了从网络骚扰、安全漏洞到勒索软件等各种严重问题。其中许多问题的根源可追溯到 IPv4 地址池短缺。

长期以来，人人平等的竞争环境一直是互联网价值主张的重要组成部分。然而，即使在基本的地址分配实践中，这也并非现实。根据世界人口[1]和当前的 IPv4 分配情况[2]，美国人均拥有 4.91 个地址，而赞比亚仅占 0.01 个，比例超过两个半数量级。梵蒂冈城人均拥有 21.44 个地址，而世界上十多个实体却一个地址也没有。这些明显的差距表明，要实现这一目标，仍有工作要做。

克服 IPv4 地址池限制的努力导致了动态寻址的使用，从根本上说，动态寻址比静态寻址要复杂得多。出于某种原因，动态机制在没有这种限制的情况下继续被用于 IPv6，而且似乎没有人质疑其合理性，这也许是因为人们普遍天真地认为动态寻址可以保护隐私和安全。实际上，只有新手入侵者才会这么想。事实上，犯罪者并不需要知道任意受害者的具体身份。另一方面，当以学校、医院、企业、政府等特定实体为目标时，它们的大部分 IP 地址都可以通过 DNS（域名系统）服务方便地查询到。严重的犯罪者利用该系统的弱点，隐藏在虚构的地址后面，在发动攻击时可以任意更改。

更糟糕的是，动态地址的做法使得对互联网流量进行取证分析变得如此困难，以至于执法部门有理由为了预防犯罪而不分青红皂白地进行大规模监控。由于没有什么可以阻止任何其他方面在具备条件的情况下采取同样的行动，归根结底，普通个人的隐私权所剩无几！这已成为一个颇具争议且错综复杂的话题 [3]。

IPv6 原本是作为改进 IPv4 的替代品，但令人大吃一惊的是，IPv6 原来并不向后兼容，这就给过渡带来了挑战，而且代价高昂。因此，有必要创建临时的双栈协议 [4]，该协议增加了成本，但并没有真正缓解原有的障碍。

端到端连接性一直是任何互联网改进建议的首要标准，但上述挑战的累积效应导致了以主从架构为特征的 CDN（内容分发网络--目前占主导地位的互联网运营模式），这种架构实际上阻碍了终端用户之间的直接点对点通信，即使在本地社区内也是如此。

互联网最初价值主张的另一部分是使公共通信系统摆脱少数几家大型电信供应商的垄断和政府机构的监管。然而，几十年后的今天，互联网服务已被分割成多个业务领域，每个领域都由一家占主导地位的跨国企业集团（和几个较小的竞争对手）提供服务，该集团实力雄厚，影响力巨大，能够逃避监管，同时对其造成的问题淡化责任。

与此同时，世界各地的主权政府越来越多地参与到互联网的日常运行中，导致互联网分裂成一个分裂的互联网[5]，对此有很多批评。事实上，IAP（互联网接入服务提供商）已将互联网架构划分为许多 AS（自治系统）[6]，需要 BGP（边界网关协议）[7]来实现互联。地缘政治分裂互联网将把单层的全球通信网络划分为多个国家片段（总数约为 195 个）[8]，而 AS 已经创建了多层（目前约有 76K 层，而且还在不断增加）[9]球形网络，每个网络都像一层完整的洋葱皮一样包裹着整个地球。从某种意义上说，这些 “洋葱网 ”层的数量几乎比潜在的 Splinternet 片段的数量多出两个半数量级。这种对比确实令人匪夷所思，即使在认识到可能的 AS 数量与 32 位 IPv4 地址池相同之前也是如此！[10]. 也许，批评 Splinternet 只是一种策略，目的是转移人们对洋葱网的注意力。

综上所述，诊断和了解互联网紧急事件的程度需要如此长的时间也就不足为奇了，而在发生恶意黑客攻击的情况下，则需要更长的时间--几天、几周、几个月甚至更长的时间--才能开始推测重大网络攻击的幕后黑手。相比之下，传统的 PSTN（公共交换电话网）甚至在电话接通之前就能确定呼叫者的位置。

总之，由于最初基于 IPv4 的互联网设计无法明确、唯一地识别世界上的每一个人，因此出现了各种动态补救措施。不幸的是，这些补救措施也为那些意图攻击合法但易受攻击用户的恶意犯罪者提供了完美的伪装。尽管新版 IPv6 的地址足以识别所有物联网（IoT），但 IPv4 临时方案仍在继续。此外，由于缺乏向后兼容性而被迫使用双协议栈方案的 IPv6 设施比纯 IPv4 更加复杂和昂贵，因此发展中地区很难采用 IPv6。这些复杂性增加了网络遭受网络攻击的可能性。然而，要迅速取代任何像互联网这样持续使用的大型系统，尤其是整个系统，是不可能的。

2. 要求：

为了打破这种僵局，现实的解决方案必须能够与当前环境共存，同时向长期系统演进。理想的方法是引入一种方案，其行为类似于现有系统的一部分--不中断正在进行的操作，但又能发展成为一个独立于基础设施运行的叠加网络，同时在两者之间保持一定距离的接口，以实现互操作性和整体服务的完整性。这将逐渐演变成两个并行运行的系统，使用相同的技术，但遵循不同的操作规范，提供类似的服务。这将使最终用户有能力亲自试验和比较两者的优缺点，以便对首选的长期配置做出明智的选择。

3. 解决方案

幸运的是，我们找到了一个紧凑的方案[11]，可以解决迄今为止讨论的大多数问题。该方案的基本方法是利用现有 CDN 构建模块 CG-NAT（运营商级-网络地址转换）中长期保留的 240/4 网

块，建立一个称为 SPR（半公共路由器）的新设施，以覆盖当前的互联网基础设施。在长期部署过程中不需要新技术。

有了足够的静态地址来识别每个用户，SPR 就不需要 DHCP（动态主机配置协议），这样 IAP 就没有分配的地址了。由于 DNS 基本上已退化为一个相当于电子电话白页的准静态数据库，而且不再需要 AS 和 BGP，因此这种新的互联网环境已大为简化。

要使用长期处于 “保留 ” 状态的 240/4 网块，可能很难找到现成的设备来测试设备能力和验证网络性能。此外，这种设备必须简洁、低成本和学习曲线最小化，以鼓励尽可能多的有关各方启动这一拟议的过渡。

下文概述了建立试验台进行实验和演示的基本设备和流程。从后者中获得的技能和经验可用于协助 SPR 的实际部署。

. **终端设备：**

Xubuntu[12]V18.04.1 被认为是最方便的操作系统（OS）候选者，因为它可以在同一台笔记本电脑（个人电脑）主机上同时承担双 IP 地址。也就是说，每台这样配备的个人电脑就像两个共享同一硬件网络端口的物联网，即一个共同的 DHCP 寻址客户端和一个静态客户端。两者都可以使用熟悉的 IPv4 或 240/4 地址。此类 PC 上的一对 IPv4 DHCP 物联网可通过传统的联网过程建立物理连接。然后，同一对个人电脑上的静态 240/4 地址物联网可验证 240/4 环境中的传输特性。在不改变任何硬件设置也不重启个人电脑的情况下，这两步测试可确保介质已准备就绪，可

传输任何一类 IPv4 地址的数据包。此外，在将新的物联网部署到现场之前，可以通过该介质将这些 PC 与新的物联网一起使用，以验证其兼容性。

. 网络模拟器：

兼容 240/4 的测试平台是鉴定兼容设备和检查其传输性能的基本结构。

A. 作为一个明确的起点，应安装 OpenWrt[13]V19.07.3 或更高版本的固件，使路由器/住宅网关（RG）完全支持 240/4。这样就可以建立内部局域网（LAN）和家庭局域网（HAN），为传统的物联网和使用 240/4 地址的物联网提供服务，同时像 240/4 DHCP 客户端一样接入互联网。

B. 为了在作为 SPR 运行的场所（以上述 RG 为代表）之间提供基本的传输结构，支持 OpenWrt 的 D-Link 智能管理型交换机 DGS-1210 系列[14]是很好的选择。

在建立 SPR 的过程中，它会形成一个覆盖网络，基本上为相同的场所提供服务，其功能与现有的 CG-NAT Fabric 相同，只是默认路由方案变成了分层路由。这一过程可以复制，最终覆盖整个 CG-NAT 集群。其次，通过充分利用 240/4 网块的大小（是 100.64/10 网块的 64 倍），可从单个 SPR 为多个 CG-NAT 集群提供服务。根据需要服务的人口规模，RAN（区域局域网）[15]可由一个或多个 SPR 组成。

4. 结论

由于 240/4 网段多年来一直被正式指定为 “保留给未来使用 ” 或 “试验性 ” 网段，因此自然会产生是否可以使用的问题。据报道，一些跨国企业集团在未发布公告的情况下，实际上已将 240/4 网块用于各种用途[16]。费了一番周折才发现这些活动的事实表明，240/4 网段的使用没有也不会干扰现有的互联网业务。因此，240/4 网段是部署建议的 SPR 的理想工具。

使用静态地址，RAN 将通过分层路由来简化互联网的运行，使公众能够享受点对点通信，而不受跨国企业集团的支配。寻址

方案的静态特性使 RAN 比现有的基于 CDN 的互联网更具有确定性，从而更能抵御网络入侵。

欲了解更多信息，请参阅在线白皮书[17]，该白皮书从更加商业化的角度分析了这一建议。

参考文献：

[1] 按人口划分的世界各国；

https://www.worldometers.info/world-population/population-by-country/

[2] 按 IPv4 地址分配的国家列表：

https://en.wikipedia.org/wiki/List_of_countries_by_IPv4_address_allocation

[3] 网络安全漏洞状况

https://blog.apnic.net/2021/02/03/the-internet-of-trash/

[4] IPv6：

https://en.wikipedia.org/wiki/IPv6

[5] 分裂互联网

https://en.wikipedia.org/wiki/Splinternet#:~:text=The%20splinternet%20(also%20referred%20to,religion%2C%20and%20divergent%20national%20interests.

[6] 自治系统

https://en.wikipedia.org/wiki/Autonomous_system_(互联网)

[7] 边界网关协议

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

[8] 世界各国

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] 当前 AS 的数量

https://thyme.apnic.net/current/data-summary

[10] 自治系统编号

https://www.arin.net/resources/guide/asn/

[11] 美国专利号 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 系列智能交换机

https://www.dlink.com/us/en/products/dgs-1210-series-gigabit-smart-plus-switches

[15] 区域网络模拟器

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] 改造互联网：

https://www.avinta.com/gallery/RevampTheInternet.pdf

术语、缩写和首字母缩略词：

. AS：自治系统

. BGP：边界网关协议

. CDN： 内容分发网络

. CG-NAT： 电信级网络地址转换

. DHCP： 动态主机配置协议

. DNS： 域名系统

. Dual-Stack 双协议栈： 支持同时使用 IPv4 和 IPv6 地址的网络环境

. HAN：家庭区域网络（用于私人/住宅的内部网络）

. IAP： 互联网接入提供商

. IoT： 物联网

. IPv4：互联网协议版本 4

. IPv6：互联网协议版本 6

. LAN： 局域网（机构使用的内部网络）

. OS： 操作系统

. PC： 个人电脑

. PSTN： 公共交换电话网络

. RAN： 区域局域网

. RG： 路由/住宅网关

. SPR： 半公共路由器

. 240/4 Netblock（240/4 网块）： IPv4 地址池，范围从 240.0.0.0 到 255.255.255.255，大约有 2.56 亿 (256M) 或四分之一亿 (0.256B)，自 1981-09 年以来一直未正式使用，因为它们被指定为 “试验性 ”或 “保留 ”供 “未来使用”。
https://www.iana.org/assignments/ipv4-address-space/ipv4-address-space.xhtml