改造互联网

1.背景：尽管互联网的迅速被采用和广泛部署已成为事实的全球通信基础设施，但对其安全漏洞的脆弱性一直困扰不已。也就是说，与传统的 PSTN 在接听电话之前就能够定位呼叫者相比，为什么互联网会花那么多的时间，几天，几个月甚至更长久才能开始猜测重大网络攻击的实施者？

造成此问题的原因是基于一个事实，即原始 IPv4 的互联网设计没有足够大的地址池来显式和唯一地标识正在使用的所有物联网点 。因此，开发了各种临时方案来动态处理此障碍。不幸的是，他们也为犯罪者提供了完美的伪装，而普通用户却像是固定靶子。尽管新版本的 IPv6 具有足够多的地址来标识所有物联网，但大家仍然持续地使用临时方案。此外，IPv6 比 IPv4 更为复杂和昂贵，这使得偏远地区采用 IPv6 非常困难。而连续使用的大型系统（例如互联网）是不能全面替换的。为了避免这种僵局，一个能与当前作法共存并同时将其改进为长期系统是唯一现实的方案。

2.解决方案：幸运的是，发现了自早期以来，IPv4 地址池有足够使用的部份（准确地说是十六分之一）被“保留”用于“将来使用”。因此，当前的互联网设备都无法使用它。这为新型路由器提供了独特的机会。可以利用它从每个现有 IPv4 地址中识别多达 2.56 亿个物网 。经过适当管理，一个完整的端到端可寻址全球通信系统不仅可以为每个用户统一提供所有服务，而且还可以减轻网络安全漏洞的根本因，而这一切都在现有 IPv4 技术的范围之内。

3.分阶段部署：240/4 网络块采用退化格式作为 192.168/16、172.16/12 和 10/8 之外的第四个专用网络地址池，可以立即部署上述方法，让当前的互联网服务器与客户端操作的模式融合在一起。在此介绍阶段仅需要启用 240/4 网络块，而无需修改现有 IPv4 设计中的任何其他内容。

4.实施：这种方法几乎不需要任何设计上的努力。部署成本与当前可比的 IPv4 设备相同。并且，由于减少了网络攻击等破坏的简化做法，运营费用将降低：

A.产品开发（ProDev）：只需禁用现有禁用 240/4 网络模块的软件代码。

B.资本支出（CapEx）：与当前具有相同的服务容量，并且使用相同的硬件的 IPv4 设备相同。

C.运营费用（OpEx）：不依赖动态方案，而通过简化的作法降低。

D.网络安全：通过确定性的物联网标识（地址）管理得到善。

5.建议的行动：

A.由于具有无需开发即可从专用网络启动互联网服务的固有特性，任何当事人（政府机构，企业，企业家等）都可以利用现有的 IPv4 设备从可用的有效 IPv4 地址中部署此提议的系统。

B.由于这种方法本质上是通用的，因此建议 ITU-D 对这个案例进行审查，以考虑其在普遍部署中改造互联网的适用性。

参考：

一。 网络安全漏洞状态

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

二。此提案的可复制性可行性证明。

https://www.avinta.com/phoenix-1/home/RegionalAreaNetworkArchitecture.pdf

三。对 IAB 博客的评论：提出此方案以促进最终用户参与协议/产品开发。

https://blog.apnic.net/2020/08/31/rfc-8890-the-internet-is-for-end-users/

四。 IETF 草案：此提案的技术细节

https://datatracker.ietf.org/doc/html/draft-chen-ati-adaptive-ipv4-address-space

五。知识产权: US Patent No. 11,159,425

术语，缩写和首字母缩写词：

- CG-NAT：运营商级网络地址转换
- DHCP：动态主机配置协议
- DNS：域名系统
- IAB：互联网体系结构委员会
- IETF：互联网工程任务组
- IoTs：物联网
- IPv4：互联网协议版本 4

- IPv6：互联网协议版本 6
- ITU-D：国际电信联盟－发展部门
- PSTN：公共交换电话网
- 240/4 网络块：IPv4 地址池，范围从 240.0.0.0 到 255.255.255.255，总计约 2.56 亿（256M）或四分之一十亿（0.256B）地址

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