改造互聯網

1.背景：儘管互聯網的迅速被採用和廣泛部署已成為事實的全球通信基礎設施，但對其安全漏洞的脆弱性一直困擾不已。也就是說，與傳統的 PSTN 在接聽電話之前就能夠定位呼叫者相比，為什麼互聯網會花那麼多的時間，幾天，幾個月甚至更長久才能開始猜測重大網絡攻擊的實施者？

造成此問題的原因是基於一個事實，即原始 IPv4 的互聯網設計沒有足夠大的地址池來顯式和唯一地標識正在使用的所有物聯網点 。因此，開發了各種臨時方案來動態處理此障礙。不幸的是，他們也為犯罪者提供了完美的偽裝，而普通用戶卻像是固定靶子。儘管新版本的 IPv6 具有足夠多的地址來標識所有物聯網，但大家仍然持续地使用临时方案。此外，IPv6 比 IPv4 更為複雜和昂貴，這使得偏远地区採用 IPv6 非常困難。而連續使用的大型系統（例如互聯網）是不能全面替換的。為了避免這種僵局，一个能與當前作法共存並同時將其改進為長期系統是唯一現實的方案。

2.解決方案：幸運的是，發現了自早期以來，IPv4 地址池有足够使用的部份（準確地說是十六分之一）被“保留”用於“將來使用”。因此，當前的互聯網設備都無法使用它。這為新型路由器提供了獨特的機會。可以利用它從每個現有 IPv4 地址中識別多達 2.56 億個物網 。經過適當管理，一個完整的端到端可尋址全球通信系統不僅可以為每個用戶統一提供所有服務，而且還可以減輕網絡安全漏洞的根本因，而這一切都在現有 IPv4 技術的範圍之內。

3.分階段部署：240/4 網絡塊採用退化格式作為 192.168/16、172.16/12 和 10/8 之外的第四個專用網絡地址池，可以立即部署上述方法，让當前的互聯網服務器與客戶端操作的模式融合在一起。在此介紹階段僅需要啟用 240/4 網絡塊，而無需修改現有 IPv4 設計中的任何其他內容。

4.實施：這種方法幾乎不需要任何設計上的努力。部署成本與當前可比的 IPv4 設備相同。並且，由於減少了網絡攻擊等破壞的簡化做法，運營費用將降低：

A.產品開發（ProDev）：只需禁用現有禁用 240/4 網絡模塊的軟件代碼。

B.資本支出（CapEx）：與當前具有相同的服務容量，並且使用相同的硬件的 IPv4 設備相同。

C.運營費用（OpEx）：不依賴動態方案，而通過簡化的作法降低。

D.網絡安全：通過確定性的物聯網標識（地址）管理得到善。

5.建議的行動：

A.由於具有無需開發即可從專用網絡啟動互聯網服務的固有特性，任何當事人（政府機構，企業，企業家等）都可以利用現有的 IPv4 設備從可用的有效 IPv4 地址中部署此提議的系統。

B.由於這種方法本質上是通用的，因此建議 ITU-D 對這個案例進行審查，以考慮其在普遍部署中改造互聯網的適用性。

參考：

一。 網絡安全漏洞狀態

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

二。此提案的可複制性可行性證明。

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

三。對 IAB 博客的評論：提出此方案以促進最終用戶參與協議/產品開發。

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

四。 IETF 草案：此提案的技術細節

https://tools.ietf.org/html/draft-chen-ati-adaptive-ipv4-address-space-08

術語，縮寫和首字母縮寫詞：

- CG-NAT：運營商級網絡地址轉換
- DHCP：動態主機配置協議
- DNS：域名系統
- IAB：互聯網體系結構委員會
- IETF：互聯網工程任務組
- IoTs：物聯網
- IPv4：互聯網協議版本 4
- IPv6：互聯網協議版本 6
- ITU-D：國際電信聯盟－發展部門

◦ PSTN：公共交換電話網

◦240/4 網絡塊：IPv4 地址池，範圍從 240.0.0.0 到 255.255.255.255，總計約 2.56 億（256M）或四分之一十億（0.256B）地址

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