Revamp The Internet

1. Background: Despite the fast adoption and the wide deployment of the Internet to become the de facto worldwide communication infrastructure, there has always been a nagging concern about its vulnerability to security breach. That is, compared to the traditional PSTN capable of locating the caller even before a call is answered, why does the Internet take so much time, days, months or even longer, to just begin speculating the perpetrator of a major cyber attack?

The cause of this issue is rooted in the fact that the original IPv4 based Internet design did not have large enough address pool to explicitly and uniquely identify all IoTs being used. Various interim schemes were developed to dynamically deal with this handicap. Unfortunately, they also provided the perfect camouflage for the perpetrators, while the ordinary users were sitting ducks in the open. Although the new version, IPv6 has more than enough addresses to identify all IoTs, somehow the use of the interim schemes persisted. Furthermore, IPv6 is more complicated and expensive than IPv4, making less-fortunate regions hard pressed to adopt IPv6. A full replacement to any continuously used large system like the Internet is out of the question. To circumvent this stalemate, a scheme that can coexist with the current practices while enhancing them toward a long term system is the only realistic venue.

2. Solution: Fortunately, it is discovered that a significant portion (one sixteenth, to be exact) of the IPv4 address pool, called 240/4 netblock has been "RESERVED" for "Future use" ever since the early days. Consequently, none of the current Internet equipment is capable of using it. This offers a unique opportunity for a new class of routers to utilize it for identifying up to 256 million IoTs from each existing IPv4 address. Properly administered, a fully end-to-end addressable worldwide communication system not only provides all desired services uniformly to every subscriber, but also mitigates the root cause of the cyber security vulnerability, all within the scope of the existing IPv4 technology.

3. Phased Deployment: To blend in with the current Internet server-client operation mode, the above approach may be deployed immediately with a degenerated format, whereby the 240/4 netblock is used as if it were the fourth private network address pool, in addition to 192.168/16,

172.16/12 and 10/8. This introductory phase only requires the enabling of the 240/4 netblock, without modifying anything else in existing IPv4 designs.

4. Implementation: This approach hardly requires any engineering effort. The deployment cost is the same as the comparable current IPv4 equipment. And, operation expenses will be lowered due to the streamlined practices that mitigate the disruptions such as cyber attacks:

A. Product Development (ProDev): Simply disable the existing software codes that have been disabling the use of the 240/4 netblock.

B. Capital Expenditures (CapEx): The same as current IPv4 equipment for the same service capacity, by using the same hardware.

C. Operation Expenses (OpEx): Lowered by streamlined practices not relying on dynamic schemes.

D. Cyber Security: Improved by deterministic IoT identification (address) administration.

5. Proposed Actions:

A. With the inherent characteristics of starting Internet services from a private network without development efforts, this proposed system may be deployed by any interested party (government agencies, businesses, entrepreneurs, etc.) from an available valid IPv4 address utilizing existing IPv4 equipment.

B. Since this approach is generic in nature, it is recommended to be reviewed by ITU-D for its suitability in universal deployment to revamp the Internet.

References:

I. Cyber security vulnerability status

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

II. A readily replicable feasibility demonstration of this proposal.

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

III. Comment to an IAB blog: Proposing this scheme to facilitate the end-user participation in protocol / product developments.

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

IV. IETF Draft: Technical details of this proposal

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

V. Intellectual Property: US Patent No.: 11,159,425

Terminology, Abbreviation & Acronym:

. CG-NAT: Carrier Grade Network Address Translation

. DHCP: Dynamic Host Configuration Protocol

. DNS: Domain Name System

. IAB: Internet Architecture Board

. IETF: Internet Engineering Task Force

. IoTs: Internet of Things

. IPv4: Internet Protocol version 4

. IPv6: Internet Protocol version 6

. ITU-D: International Telecommunication Union – Development Sector

. PSTN: Public Switched Telephone Network

. 240/4 Netblock: IPv4 address pool ranging from 240.0.0.0 to 255.255.255.255, amounting to roughly 256 Million (256M) or quarter of a Billion (0.25B) addresses

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