Streamline The Internet

1. Background:

The rapid adoption and wide deployment of the Internet to become the de facto worldwide communication backbone has been accompanied by issues ranging in severity from cyber harassment to security breaches to ransomware. The origin of many of these issues may be traced to the IPv4 address-pool shortage.

A level playing field for all has long been a big part of the Internet's value proposition. However, this is not a reality even in the basic address-allocation practice. Based on the world's population [1] and current IPv4 allocation [2], the US has 4.91 addresses per capita, while Zambia's share is only 0.01, a ratio in excess of two-and-one-half orders of magnitude. Vatican City has 21.44 per capita while over a dozen entities of the world have none. These stark discrepancies make it clear that much still remains to be done to achieve the goal.

Efforts to overcome IPv4 address-pool limitations led to the use of dynamic addressing, which is fundamentally much more involved than its static counterpart. For some reason, dynamic mechanisms continue to be used with IPv6 in the absence of such limitations, and no one seems to question the rationale, perhaps because of a common naive belief that dynamic addressing protects privacy and security. In reality this turns out be true only with novice intruders. The fact is that perpetrators do not need to know the specific identification of an arbitrary victim. On the other hand, when targeting specific entities such as schools, hospitals, businesses, governments, etc., most of their IP addresses are readily available through the DNS (Domain Name System) service for facilitating inquiries. Serious perpetrators exploit the weaknesses in the system by hiding behind fictitious addresses that can be changed arbitrarily when they launch their attacks.

Worse yet, the dynamic-address practice has made it so difficult to perform forensic analyses of Internet traffic that it justified indiscriminate mass surveillance by law enforcement for the sake of crime prevention. Since there is nothing to stop any other party from doing the same, if so equipped, there is in the final analysis little, if any, privacy left for ordinary individuals! This has become quite a controversial and convoluted topic [3] .

Intended as a replacement for improving IPv4, it came as a great surprise that IPv6 turned out not to be backward compatible, making for a challenging and costly transition. It necessitated the creation of the interim Dual-Stack Protocol [4] that increased cost while not really relieving much of the original handicap.

End-to-end connectivity has always been imposed as the first criterion on any proposed Internet improvements, but the cumulative effect of the above challenges has led to a CDN (Content Delivery Network - the currently predominant Internet operation model) characterized by a master-slave architecture that actually impedes direct peer-to-peer communication among end-users, even within a local community.

Another part of the original value proposition of the Internet was to free public communication systems from being monopolized by a few big telecommunications providers and from regulation by governmental agencies. Decades later, however, Internet service is now segmented into several business sectors, with each served by a single dominant multi-national conglomerate (and a few smaller competitors) that is so powerful and influential that it is able to evade regulations while downplaying responsibility for issues it creates.

At the same time, there is much criticism of the increasing involvement of sovereign governments worldwide in daily Internet operations as leading to the fragmentation of the Internet into a Splinternet [5]. The fact is that IAPs (Internet Access Providers) have partitioned the Internet architecture into many ASes (Autonomous Systems) [6] requiring BGP (Border Gateway Protocol) [7] to interconnect them. The geo-political Splinternet would divide a single-layer worldwide communication network into national fragments (total of about 195) [8], while the ASes have already created layers (currently around 76K and growing) [9] of spherical networks, each enveloping the entire globe like one complete layer of onion peels. In a certain sense, the number of these “Onion-net” layers is nearly two-and-one-half orders of magnitude greater than that of potential Splinternet fragments. This contrast is truly mind-boggling, even before recognizing that the number of possible ASes is the same as the 32 bit IPv4 address pool! [10].

Perhaps criticizing the Splinternet is a tactic to distract attentions from focusing on the Onion-net.

When all of the above is taken together, it is not surprising that so much time is required to diagnose and understand the extent of an emergency Internet event, and even more so in the event of a malicious hack - days, weeks, months or even longer - to just begin speculating about the party behind a major cyber attack. By comparison, the traditional PSTN (Public Switched Telephone Network) is capable of locating the caller even before a call is answered.

In summary, the inability of the original IPv4-based Internet design to explicitly and uniquely identify every person in the world led to various dynamic remedies. Unfortunately, these remedies also provided the perfect camouflage for malicious perpetrators intent on attacking legitimate but vulnerable users. Although the new version IPv6 has more than enough addresses to identify all IoTs (Internet of Things), the IPv4 interim schemes continue to be perpetuated. Furthermore, the IPv6 facility, forced to use the Dual-Stack scheme due to the lack of backward compatibility, is more complicated and expensive than pure IPv4, with the result that developing regions are hard pressed to adopt IPv6. These complexities increase network vulnerability to cyber attacks. Nevertheless, a quick replacement of any continuously used large system like the Internet, especially in its entirety, is out of the question.

2. Requirement:

To circumvent this stalemate, a realistic solution must be able to coexist with the current environment while evolving toward a long-term system. The ideal approach would be to introduce a scheme that behaves like part of the existing system - with no disruption to ongoing operations - but has the ability to evolve into an overlay network that functions independently of the base facility, while maintaining arm’s-length interfaces between the two for interoperability and overall service integrity. These would gradually evolve into two systems operating in parallel, using the same technology, but following different operational disciplines to deliver comparable services. This would empower end-users to personally experiment and compare the pros and cons of both in order to make an informed choice for the preferred long-term configuration.

3. Solution:

Fortunately, a compact scheme [11] that can deal with most of the issues discussed so far has been identified. The basic approach of this scheme is to utilize the long-reserved 240/4 netblock in the existing CDN's building block, CG-NAT (Carrier Grade - Network Address Translation) for establishing a new facility, called SPR (Semi-Public Router), to overlay the current Internet infrastructure. No new technology is required in the process of such a deployment over time.

Having enough static addresses for identifying every user, an SPR needs no DHCP (Dynamic Host Configuration Protocol) which leaves IAPs no allocated addresses to assign. With DNS essentially degenerating to a quasi-static database equivalent to an electronic telephony White Pages and AS and BGP are no longer needed, this new Internet environment is much simplified.

To use the 240/4 netblock that has been in the "Reserved" status for so long, it may be difficult to find readily available equipment for testing the device capability and verifying the network performance. Also, such a facility must be greatly simplified, low cost and minimal in its learning curve in order to encourage as many interested parties as possible to kick off this proposed transition.

The following outlines the basic equipment and process to set up a test bed for experiments and demonstrations. The skills and experience gained from the latter can then be applied to assist the actual SPR deployment.

. Terminal Instrument:

Xubuntu [12] V18.04.1 has been identified as the most convenient OS (Operating System) candidate because it can assume dual IP addresses simultaneously on the same host notebook PC (Personal Computer). That is, each such equipped PC behaves like two IoTs sharing the same hardware network port, namely, a common DHCP addressed client alongside a static one. Both can assume either the familiar IPv4 or the 240/4 address. A pair of IPv4 DHCP IoTs on such PCs can establish the physical connectivity between them via the conventional networking process. Then, the static 240/4 addressed IoTs on the same pair of PCs can verify the transmission characteristics in the 240/4 environment. With no changes to any hardware setup nor rebooting of the PCs, this two-step test assures that the medium is ready for transporting packets with any IPv4 address in either category. In addition, these PCs may be used with a new IoT through this medium to verify its compatibility before deploying it to the field.

. Network Simulator:

A 240/4-compatible test bed serves as the basic fabric for qualifying compatible devices and checking their transmission performance.

A. For a definitive starting point, an RG (Routing/Residential Gateway) should be made fully 240/4 capable by installing OpenWrt [13] firmware V19.07.3, or higher, which supports a long list of commercial RGs. This will establish on-premises LANs (Local Area Networks) and HANs (Home Area Networks) that serve both traditional IoTs and those assuming 240/4 addresses, while behaving like 240/4 DHCP clients to the Internet.

B. To provide a basic transmission fabric among premises (represented by the above RGs) operating as an SPR, the OpenWrt supported D-Link smart managed switch DGS-1210 Series [14] are good candidates.

While an SPR is building out, it forms an overlaying network that essentially serves the same premises with the same functions as the existing CG-NAT fabric, except the default routing scheme becomes hierarchical. This process may be replicated to eventually overlay an entire CG-NAT cluster. Next, multiple CG-NAT clusters may be served from one single SPR by taking full advantage of the 240/4 netblock size which is 64 times that for a 100.64/10 netblock which sets the limit on the capacity of a CG-NAT cluster without dynamic reassignment. Depending on the size of population to be served, an RAN (Regional Area Network) [15] may consist of one or more SPRs.

4. Conclusion:

Since the 240/4 netblock has been formally designated as “Reserved for Future Use” or “Experimental” for so many years, questions naturally arose about whether it could be used. Multi-national business conglomerates have been reported to be actually using the 240/4 netblock for various purposes without announcements [16]. The fact that it took some effort to discover such activities indicates that use of the 240/4 netblock does not and will not disrupt existing Internet operations. So, the 240/4 netblock is an ideal vehicle for deploying the proposed SPR.

Using static addresses, the RAN will streamline Internet operation via hierarchical routing that empowers the general public to enjoy peer-to-peer communication, free from dominance by multi-national business conglomerates. The static nature of the addressing scheme enables the RAN to be more deterministic than the existing CDN based Internet, and thus more robust against cyber intrusions.

For more information, there is an online whitepaper [17] that analyzes this proposal from a more business oriented perspective.

References:

[1] Countries in the world by population;
https://www.worldometers.info/world-population/population-by-country/

[2] List of countries by IPv4 address allocation:
https://en.wikipedia.org/wiki/List_of_countries_by_IPv4_address_allocation

[3] Cyber security vulnerability status
https://blog.apnic.net/2021/02/03/the-internet-of-trash/

[4] IPv6:
https://en.wikipedia.org/wiki/IPv6

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

[6] Autonomous System
https://en.wikipedia.org/wiki/Autonomous_system_(Internet)

[7] Border Gateway Protocol
https://en.wikipedia.org/wiki/Border_Gateway_Protocol

[8] Countries in the world
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] Number of Current ASes
https://thyme.apnic.net/current/data-summary

[10] Autonomous System Numbers
https://www.arin.net/resources/guide/asn/

[11] US Patent No. 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 Series Smart Switches
https://www.dlink.com/us/en/products/dgs-1210-series-gigabit-smart-plus-switches

[15] Regional Area Network Simulator
https://www.avinta.com/gallery/RegionalAreaNetworkSimulator.pdf

[16] Using 240/4 Unannounced
https://labs.ripe.net/author/qasim-lone/2404-as-seen-by-ripe-atlas/

[17] Revamp The Internet:
https://www.avinta.com/gallery/RevampTheInternet.pdf

Terminology, Abbreviation & Acronym:

. AS: Autonomous System

. BGP: Border Gateway Protocol

. CDN: Content Delivery Network

. CG-NAT: Carrier Grade Network Address Translation

. DHCP: Dynamic Host Configuration Protocol

. DNS: Domain Name System

. Dual-Stack: A networking environment that supports the simultaneous use of both IPv4 and IPv6 addresses

. HAN: Home Area Network (On-Premises network for private/residential parties)

. IAP: Internet Access Provider

. IoT: Internet of Thing

. IPv4: Internet Protocol version 4

. IPv6: Internet Protocol version 6

. LAN: Local Area Network (On-premises network used by institutions)

. OS: Operating System

. PC: Personal Computer

. PSTN: Public Switched Telephone Network

. RAN: Regional Area Network

. RG: Routing/Residential Gateways

.	SPR:	Semi-Public Router

.	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 (0.256B) addresses that have not been in formal use since 1981-09 because they were designated as “Experimental” or “Reserved” for “Future use”.

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