IPv6 Myth
&
Internet Vs PSTN

Table of Contents

1. Introduction

As soon as the Internet became popular, talk began to spread that its assignable IPv4 address pool would be exhausted before too long[1]. Two companion technologies were utilized in the RG (Residential Gateway) to ease this pressure, 1) NAT (Network Address Translation)[2] and 2) DHCP (Dynamic Host Configuration Protocol)[3]. NAT enables multiple host devices (each could even have multiple sessions) on a private

[1] IPv4 Address Exhaustion: http://en.wikipedia.org/wiki/IPv4_address_exhaustion
[2] Network Address Translation: http://en.wikipedia.org/wiki/Network_address_translation
[3] Dynamic Host Configuration Protocol: http://en.wikipedia.org/wiki/Dynamic_Host_Configuration_Protocol

network to share a common Internet address by assigning a Port number to each session, thus reducing the demand for the public IP addresses[4]. DHCP relieves the burden of manually setting up multiple host devices (each with a set of numerical parameters, although most are part of a local template, thus prone to typos) on the same private network. ISPs (Internet Service Providers) also took advantage of DHCP technology to conserve their allocated IPv4 addresses by normally only assigning dynamic addresses, reserving the static addresses for premium paying subscribers.

Nevertheless, it was reported that the IPv4 pool would soon be exhausted anyway. IPv6 was thus developed and then put into use. It turns out that IPv6 is not a superset of IPv4 and is not capable of encapsulating IPv4 packets. As a result, the two systems have been running side by side, prompting the merits of IPv6 to be debated ever since[5]. The current general prediction is that both protocols will be in coexistence for quite some time to come. Recently, it was announced that the IPv4 pool has been fully allocated[6] and reports even began to surface that a certain allocated IPv4 address block has been exhausted[7].

The message commonly conveyed to the general public is that the main motivation for using IPv6 is to create a big enough addressing pool for the upcoming IoT (Internet of Things), whose requirements will exceed the IPv4 capability. However, in the publicly available literature, quantitative justification of this need has been lacking. What is unclear is the relationship between the projected number of IoTs and the IPv4 addressing capacity. This document will provide a high-level analysis of this relationship that is based on functional logic, system architecture, available technology and public data, without being confined by current actual practices and specific technical implementations, so that a generic baseline may be established.

Other proposed reasons for going to IPv6 include potential benefits such as better performance that results from features like enabling end-to-end connectivity through direct addressing and improved security without being more complicated than IPv4, so that connected devices are not burdened. These topics are secondary to the IPv4 exhaustion issue, yet closely related to the overall considerations and principles employed by the Internet that may influence the outcome. The lack of consistent and concise definitions and rationale in the public domain fuels the confusion further[8]. This paper will attempt to briefly address these topics individually. Where interactions do exist, we will cross reference to one another as appropriate.

---

[4] How Network Address Translation works; http://computer.howstuffworks.com/nat.htm
[5] IPv6: http://en.wikipedia.org/wiki/IPv6
[6] IANA IPv4 Address Space Registry: http://www.iana.org/assignments/ipv4-address-space/ipv4-address-space.xhtml
[7] IPv4 Exhaustion Gets Real – Microsoft Runs Out Of U.S. Addresses For Azure Cloud – Time to Move To IPv6!: http://www.internetsociety.org/deploy360/blog/2014/06/ipv4-exhaustion-gets-real-microsoft-runs-out-of-u-s-addresses-for-azure-cloud-time-to-move-to-ipv6/
[8] IPv6 Addressing, Subnets, Private Addresses: http://www.networkworld.com/article/2228449/microsoft-subnet/ipv6-addressing--subnets--private-addresses.html

One important, basic philosophical issue deserves to be mentioned before proceeding with the specifics. A most puzzling aspect behind ongoing discussions is that the broadband industry, in general, appears to have taken the position that what it calls broadband communications is different from traditional communications. As a result, the experience gained over a century of the PSTN (Public Switched Telephone Network) is mostly irrelevant to Internet issues. Since the Internet is poised to assume most, if not all, services that have been provided by the PSTN, mirroring each other probably would be the most prudent approach for ensuring a smooth transition. Without a working tried-&-true legacy system as a template to check against, everything has to be regarded as new and subject to the steep learning curve of trial and error. Disregarding the learning from the past seems to be an unnecessary waste of resources. In the report below, we will utilize well-established PSTN principles, disciplines, practices and conventions, etc. as comparison yardsticks in analyzing Internet issues. It will become apparent that such analogous comparisons help us to streamline the logic for a more consistent overall perspective of public communication systems.

2. Myth 1: IPv4 Address Pool Is Not Enough

To comprehend the IPv4 address pool exhaustion issue, one must first know how many communicating devices are to be accounted for. A recent Cisco online paper[9] provides the most up-to-date forecast that by Year 2020 worldwide population will be 7.6 billion, while IoT in use will be 50 billion.

A. This means that on average, each person will be using 6.58 IoTs. This last number appears to be on the high side. However, for the purpose of this analysis, a higher requirement provides the result of our resource allocation with a better safety margin.

B. The IPv4 dot-decimal address format, consisting of four octets each made of 8 binary bits, results in the maximum number of assignable public addresses of 4.295 billion (calculated by 256 x 256 x 256 x 256, to be 4,294,967,296 – decimal exact). Using the binary notation of 64K representing 256 x 256 (decimal 65,536), the full IPv4 address pool of 64K x 64K may be expressed as 4,096M, or 4.096B. Since the significant digits of the binary notation are smaller than, while its order of magnitude is the same as, the actual values in decimal format, we can safely use this conservative binary format for presenting resources in the discussions below. At first glance, it does seem that 4.096B addresses definitely are not enough to identify the expected population of 7.6 billion, let alone the 50 billion IoTs. Peering just below the surface, however, the opposite may be true.

C. Row "192.0.0.0/8" in the “List of Assigned 8/ IPv4 Address Blocks”[10] states that the entire address block of 192.168.0.0/16 representing 64K (256 x 256) addresses is reserved for use on private networks such as business LAN (Local Area

[9] The Internet of Things How the Next Evolution of the Internet is Changing Everything: https://www.cisco.com/web/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf

[10] List of Assigned 8/ IPv4 Address Blocks: http://en.wikipedia.org/wiki/List_of_assigned_/8_IPv4_address_blocks

Network) and residential HAN (Home Area Network). This is well-known by the technical community and even many consumers.

D. An interesting fact is while reserving this block of 64K addresses from the overall IPv4 address pool is insignificant because it is merely one 64Kth of the overall address pool, allocating it to be re-usable over the private network behind each remaining public IPv4 address means that the overall identifiable devices may now be multiplied from 4.096B by 64K to become 262,140B. This is 5200 times more than the expected Year 2020 IoT devices (50 billion). This significant margin for identifying IoT, while the basic public address pool is insufficient for the expected population, suggests that the IPv4 address pool capacity issue may be resolved by optimizing the boundary line between public and private network in the address space. This could be realized by redefining the usage of the already allocated 192.168.0.0/16 block.

3. Parsing Private Network Address Block

A. Since 64K addresses in the currently allocated 192.168/16 private network address block are too many for most, if not all, individual private entities to effectively utilize, let us parse it between the third and the fourth octet into two levels of addressing, each consisting of 256 choices.

B. The third octet of 192.168.0/24 may be designated as re-usable semi-public addresses behind each original IPv4 public address. This results in 1048.576B (4.096B x 256) combined public and semi-public addresses that are more than 137 times of the expected Year 2020 world population (7.6 billion). Note that with this "Extended" IPv4 public Address Pool now capable of identifying every individual of the world population, each Internet user may be assigned with a static IP address. Essentially, every person can have a permanent identification number for life. There is no more need for DHCP service in the public domain.

C. Next, each individual may use the 256 combinations from the fourth octet of 192.168.nnn.0/32, where "nnn' is determined by the process of the last step, to identify the 6.58 IoTs that (s)he may have. Similarly, this allocation is 38 times more than the projected average need.

D. Since the above proposed Extended IPv4 public addresses are much more than needed to identify the world population, we could cut back this pool by starting it with only $1/16^{th}$ of the original IPv4 address blocks. The resultant 65.536B Extended IPv4 public addresses are still more than 8.6 times of the expected Year 2020 population. In addition, a household usually is shared by a few people. The actual entities that need be publicly addressed will be a fraction of the population. So, this population based public address pool has additional built-in safety margin.

E. Note that the above derivation is intended for ordinary consumers. Savvy users having a large number of IoTs may instead utilize two lesser-known blocks, 10/8

and 172.16/12 with the capacity of 16M and 1M addresses, respectively[11], allocated for private institution use. As a mater of the fact, if either of these two address blocks is utilized, instead of 192.168/16 (64K address capacity), for the proposed approach, the resultant Extended IPv4 public address pool capability could also be significantly larger than that outlined here.

F. For example, there is a proposal to IETF called EnIP (Enhanced IP) that utilizes the 10/8 block to increase the assignable addresses[12],[13].

a. Each EnIP address has 8 octets (8 bytes or 64 bits), consisting of two full IPv4 addresses, one from the public pool and the other from the b business 10/8 block. EnIP transports the extra 4 byte addresses on either end of a connection with a 4 bytes option identifier, resulted in a 12 bytes overhead as compared to the basic IP Header.

b. Each ExIP address has 5 octets (5 bytes or 40 bits), consisting of one public IPv4 address plus one "Extension" address (third octet of 192.168.nnn/24). With shorter addresses, only 4 bytes overhead is needed in ExIP Header. Since IP Header is made of 4 bytes (32 bits) words, the ExIP Header uses only one word overhead.

c. A preliminary Draft for IETF RFC (Request For Comments) details the process of how IP packet header may be modified to accommodate the above ExIP scheme[14]. It turns out that utilizing the same mechanism, ExIP working in conjunction with EnIP may offer a wide range of IPv4 address options, besides mitigating the shortage issue.

4. Implementation

A. Although allocated with 192.168/16, current private network devices are commonly identified by 192.168.mmm.0/32 addresses, where "mmm" = 1 or 2 most of the time, according to the respective manufacturer's preference. Thus, implementing the proposal above does not impose much of a burden on these deployed private network products at all.

B. The 192.168.0/24 semi-public addressing scheme conceptually requires a new layer of distributed routers which may be made of common RGs provisioned accordingly, and without NAT function. Each router serves a relatively small local cluster of up to 256 subscribers, such as an apartment complex, a high-rise building, a block of houses, etc. For larger entities of this kind, two or more of these semi-public routers may be employed to handle the desired number of subscribers.

[11] Private IPv4 Address Spaces: http://en.wikipedia.org/wiki/Private_network
[12] IPv4 with 64 bit Address Space: http://tools.ietf.org/html/draft-chimiak-enhanced-ipv4-00
[13] Enhanced IP: http://www.enhancedip.org/docs/enip.pdf
[14] Preliminary Draft to IETF RFC – ExIP: http://www.avinta.com/phoenix-1/home/IETF-Draft-ExIP.pdf

C. Note that the boundary of a private network under this proposed Extended IPv4 address scheme will be confined within each 192.168.nnn.0/24, where "nnn" is assigned by a semi-public router. The NAT function in RGs will be lowered by one octet to this level, thus relaxing the demand on its capacity related performance.

D. Essentially, the current RG design may be used for routing either the third or the fourth octet of the 192.168/16 private address block with the actual functions customized to one of the two levels upon deployment.

E. Figure 1 below graphically depicts a possible architecture that extends the assignable IPv4 address pool in order to realize this proposal.

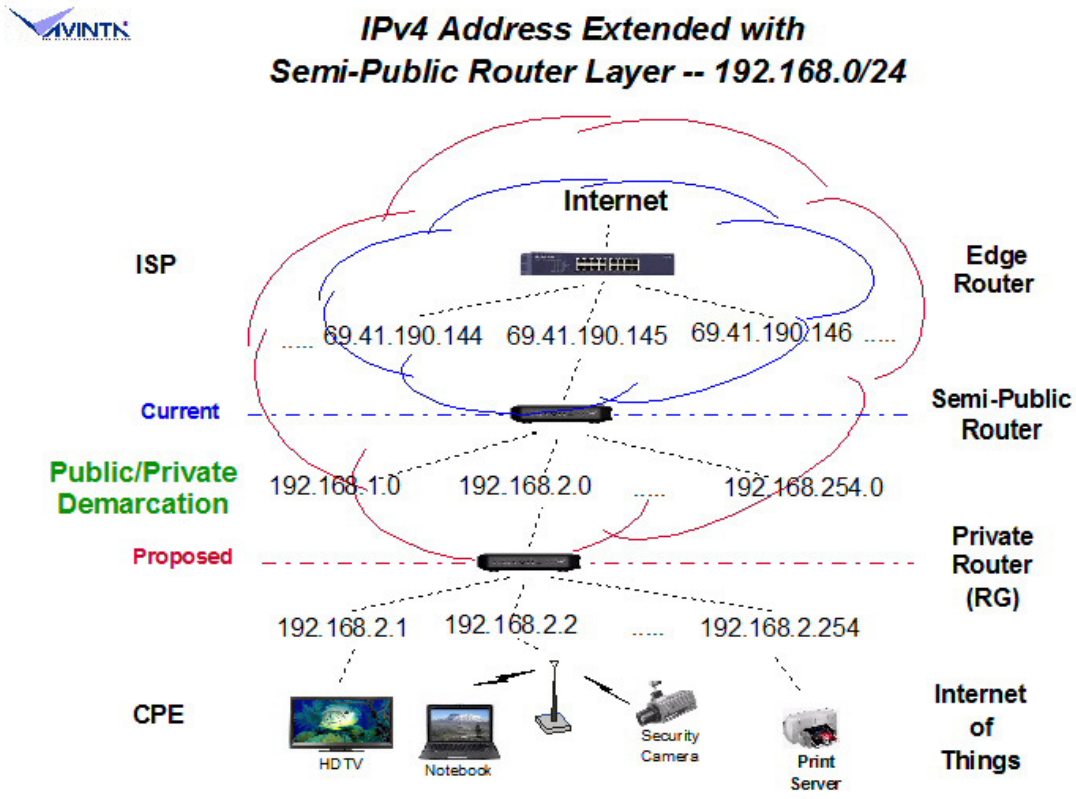

Figure 1

a. Since the physical connection hardware to respective subscribers already exists at the current edge router, and the semi-public router provides just one extra stage of simple routing, the latter could be absorbed, through software enhancement, into the former.

b. The existing RG Router may remain in place, and it is reduced to routing only the 4th octet of 192.168.nnn.0/32, where "nnn" is assigned by the host semi-public router.

c. Overall, the implementation could consist of merely edge router software enhancements. There might not be any need for new, or upgrades to existing, hardware.

d. Since each customer premises is identified by the third octet "nnn" of the 192.168.nnn/24 under a regular IPv4 address assigned by ISP, only "nnn" part (one octet, one byte or 8 bits) needs be appended to an IPv4 address to uniquely identify a premises.

e. For example, the customer premises in the diagram populated with IoTs may use 69.41.190.145 – 2 to identify itself to other Internet users.

F. Upon examining the latest IPv4 allocation, it appears that there are sixteen contiguous highest-level address blocks (240/8 through 255/8) reserved for future use[15]. These will be the ideal resource for accommodating the proposed transition from the current IPv4 allocation. Even if some of these have already been assigned, there is time to reclaim them because the incident proposal is geared for the Year 2020 projection. As a matter of fact, for the short term, each of the currently allocated IPv4 addresses may be immediately extended by 256 times with the 192.168.nnn/24 semi-public address scheme anyway. This will result in much more than the 50B needed to serve all IoTs by 2020. As long as the routing down to this level maintains the current practice of using a DHCP server to assign IP addresses to RGs, subscribers will not sense any change during the transition.

G. After completing the proposed transition, the entire 15/16th of the original IPv4 public address pool (address blocks 000/8 through 239/8) will become available for new assignments. This is a bonus consequence. We can take advantage of this to further expand the overall IPv4 public address usage. Figure 2 outlines a possible transition plan to an ExIP-based address pool lineup. Note that the choice of specific /8 blocks is just for illustrating the concepts. They may be selected to ease the transition from current assignments.

a. Group 0: To provide immediate relief to the IPv4 public address shortage issue, extend any currently assigned public address in the 000/8 - 239/8 range, wherever needed, by using 192.168.nnn/24 semi-public routers. Since this approach only requires an upgrade to Internet edge-router software, it should be transparent to already deployed RGs. This is a preparatory step for facilitating the transition to the long-term allocations.

[15] IANA IPv4 Address Space Registry: http://www.iana.org/assignments/ipv4-address-space/ipv4-address-space.xhtml

b. Group 1: Systematically port all of the above to the reserved 240/8 - 255/8 range and extend each with 192.168.nnn/24 semi-public router. This should free up the entire 000/8 - 239/8 blocks for new applications. Following a top-down structure with geographic locality information encoded to the greatest level of detail possible, this new allocation can be very compact even as it facilitates normal routing while discouraging DoS (Denial of Service) attacks. This is the primary Group of ExIP addresses for moving forward.

c. Group 2: Savvy users with a lot of IoTs could request the freed-up 000/8 - 015/8 range addresses, each extended with 172.16/12 private network routers capable of a much bigger (1M) reusable private address pool.

ExIP Transition Outline

Group	Recommended IPv4 Public Address Blocks	IPv4 Public Address Pool	Reserved Private Network Address Blocks	Proposed Semi-Public Routing	Semi-Public Address Pool Extension	Publicly Addressable Entities	IoTs on each Private Network	No. of Identifiable Addresses
0	000/8 - 239/8	3.84B	192.168/16	192.168.nnn/24	x 256	983.04B	256	251,658B
1	240/8 - 255/8	0.256B	192.168/16	192.168.nnn/24	x 256	65.54B	256	16,777B
2	000/8 - 015/8	0.256B	172.16/12	172.16.nnn/20	x 256	0.256B	4K	256,000B
3	016/8 - 031/8	0.256B	10/8	10.nnn/16	x 256	0.256B	64K	4,096,000B
4	032/8 - 239/8	3.328B	(Direct Public Addresses)			3.328B	-----	3.328B

Notes:

A. IP Address "Extension Number"

nnn = 0 - 255

B. 192.168.0.0/32 Bit Usage

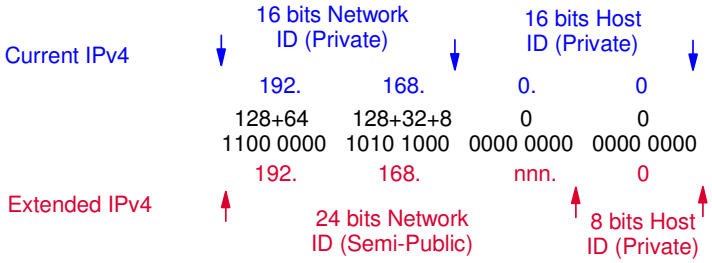

Figure 2

d. Group 3: Large organizations such as government, corporations, etc., could request the freed-up 016/8 - 031/8 range addresses, each extended with 10/8 private network routers capable of an even bigger (16M) reusable private address pool.

e. The proposed semi-public routing technique may be applied to Groups 2 & 3 by partitioning private business address 10/8 and 172.16/12 blocks, respectively, to add more flexibility in address assignment. Since these two blocks, as well as 192.168/16, are under separate groups of /8 IPv4 public addresses, there is no need to transport in each IP header their leading "template" bits to distinguish them from one another.

f. Group 4: Upon completing the porting of Group 0 to Groups 1, 2 and 3, the 032/8 - 239/8 blocks will become available for allocations in those applications requiring direct IPv4 addresses.

g. Note that Groups 2 & 3 probably do not need as many /8 blocks as Group 1. The excess address blocks should be reclaimed to increase the Group 4 address pool.

h. To maximize the use of the resources, reserve 16 blocks of /8 addresses for future use and then spread the remainder of Group 4 to Group 1. In so doing, there will be more spares available to buffer among geographic subgroups.

5. Myth 2: IPv6 Restores End-To-End Connectivity

The second major benefit promised by IPv6 has to do with restoring the end-to-end, or host-to-host, connectivity through the Internet, originally envisioned by IPv4. Since all current broadband devices, both on private networks and those directly connected to the Internet are able to access web services, and accessing those with public addresses has been functioning as planned, this particular topic may be narrowed down to just the case of accessing devices on private networks from the Internet, or the so-called inbound packet requesting to start a new session. With NAT in popular use, this last case is essentially blocked. However, techniques such as DMZ (De-Militarized Zone)[16] have made it possible to forward un-invited packets to designated devices, such as the web server of a business, to respond. The DMZ subsystem may be enhanced to forward initial connect request packets to different devices according to the following scenario:

A. If the payload has no private IP address matching that of a valid destination device, the packet is dropped.

B. Only when the destination private IP address in the payload matches with one of the active devices, will DMZ forward the packet to that devise. When that device responds, an outgoing packet with a Port number assigned by the NAT will establish a new session for the remote device to follow up. From here on, the DMZ function is bypassed so that communication may proceed unimpeded. Thus, it appears that end-to-

[16] DMZ (computing): http://en.wikipedia.org/wiki/DMZ_%28computing%29

end connectivity is already possible under existing IPv4 addressing scheme. The one additional extra step during the routing of the initial request packet is a minor event that should not be regarded as a performance issue.

C. Of course, the unpredictability of active IP addresses due to current private network DHCP practice does introduce another twist. However, this uncertainty may be eliminated by a simple manual process[17] which enables private network device addresses to remain static as long as the premises owner wishes, so that they may be distributed to welcomed remote parties, starting from IoT's owner on the road, to initiate a session.

The basic purpose of the NAT and DMZ combination described here is to facilitate the initial connection request. This pair also may serve as part of a network's rudimentary security measures. In "Myth 4", we will discuss its contribution to defend a private network.

6. Precedence & Parallelism

Although the above proposal for relieving the IPv4 pool shortage by creating a layer of semi-public routers may sound new, there is a strong resemblance to what occurred in the telephony industry. Looking at it further from this angle, a list of parallel cases between PSTN and Internet can be identified. Depending on an individual reader's background, these correlations may appear fairly obvious on the one hand to stretching the imagination on the other. To maintain the flow of this report, however, such analysis and examples are presented in the Appendix.

7. Related Topics

The following few topics are not directly associated with the IPv4 address pool size issue. Yet, they may have something to do with the philosophy behind the Internet that affects the effectiveness of IP address assignment or operation.

A. Myth 3: Direct accessing IoT improves performance

In principle, this is true because of the end-to-end connection. And, NAT used by IPv4 does slow down the session setup somewhat. However, does this degradation really matter for IoTs which are IPv6's primary targets? IoTs are being promoted as simple devices each with a specific function around a home. Normally, they are not expected to communicate with high performance. In fact, most of them need justification for having Internet connectivity. Now that the ExIP scheme has made enough direct IPv4 public addresses available, performance intensive IoTs may, if needed, request such facility to achieve the service goal. Most IoTs probably will do just fine using the proposed ExIP scheme to deliver ordinary performance.

[17] User Settable Unified Workstation Identification System: US Patent No. 6,721,790

B. *Myth 4: IPv6 improves security*

Internet security can be very sophisticated. For example, TOR (The Onion Router) [18] freeware enabling online anonymity that even got the NSA (National Security Agency) involved. Instead of building Fort Knox[19] around IoTs which, by nature are simple consumer oriented devices, it would seem that rudimentary measures functioning like an improved combination lock to reduce the predictability of active IP addresses would be sufficient to discourage non-professional intruders.

Communication security consists of three components - encrypting the payload, screening / blocking the intruder and tracing back to the perpetrator.

a. Encryption for security is often mentioned as a justification for IPv6. However, the general opinion seems to be that there is not much difference in this respect between IPv4 and IPv6, except that IPsec[20] is optional for IPv4, but mandatory in IPv6.

b. NAT does the job of blocking intruders well, but has been accused of breaking up the IPsec function[21]. However, this conflict may be because the definition of the encryption/decryption pair is between end-to-end hosts or IoTs. If, instead, the pair is defined to be between the RGs of the two communicating premises, there will be no NAT in the way of the encryption mechanism.

As mentioned earlier under "Myth 2", NAT may be teamed with DMZ to direct legitimate initial connect request packets to appropriate IoTs on a private network. With respect to security, such a configuration also imposes extra efforts on the hacker so that the chance for detecting attempted breach is improved. These measures consist of the following elements. They are either already in place or simple to implement.

i. Make use of the NAT capability at the RG, so that IoTs on a LAN or HAN are not directly accessible from the Internet.

ii. Instead of using factory preset DHCP servers in RGs that make address assignment behavior common knowledge, a premises owner may manually set IoT identifications from the available 256 choices of the 192.168.n.0/32 address block[22].

iii. The last step may be made a little bit more sophisticated by letting the owner pick a personal code for each room and then allowing a local DHCP server to carry out the detailed assignment task[23] to the IoTs in the same room. In

[18] TOR (Anonymity network): http://en.wikipedia.org/wiki/Tor_%28anonymity_network%29
[19] Fort Knox: http://en.wikipedia.org/wiki/Fort_Knox
[20] IPsec: http://en.wikipedia.org/wiki/IPsec
[21] IPv4 address exhaustion: http://en.wikipedia.org/wiki/IPv4_address_exhaustion
[22] User Settable Unified Workstation Identification System: US Patent No. 6,721,790
[23] Connected Digital Home – Build From Ground Up, Page 4 - HAM (Home area network Access Manager): http://www.avinta.com/phoenix-1/home/DigitalHome-BuildFromGroundUp.pdf

this process, optional algorisms may be employed to randomize / spread the reusable 256 choices before allocating them to each DHCP server to assign.

iv. During operation, DMZ pre-screens a connect request packet before forwarding it on to the private network. Detection of a mismatched destination IP address from an initial connect request packet would turn on a re-triggerable time-out mechanism in the DMZ which stretches the time to wait before the next connection request is allowed, thus frustrating the hacker.

v. Note that a similar strategy may be applied to a local request toward a correct IoT. This strategy will cause all other IoTs on the same network segment to turn on the defense mechanism, for example against the intrusion via wireless access. Since the probability of two consecutive valid connection requests directed to two active IoTs occurring closely is very low for the small LAN or HAN environment, this screening process should not be noticeable by the IoT user. This technique has been successfully implemented in a piece of consumer telephony equipment that is the building block for a dPABX (distributed PABX)[24].

vi. Upon detecting consecutive mismatched connect requests exceeding a preset limit, the DMZ or an IoT may send an intrusion alert to a monitor that is plugged into the local LAN / HAN[25], or a central service in the Internet, to begin proactive defensive actions such as tracing back the requesting packets to identify the intruder.

c. The tracing back to the perpetrator turns out to be not a straightforward process, likely due to the current IP address format lacking locality information. It appears that neither IPv4 nor IPv6 address formats have such information. Each Internet institution may assign its allocated block of addresses to subscribers who could be at any corner of the globe. Essentially, from the address map perspective, the Internet currently consists of many overlapping global networks each with only the responsible institution identified to be within a country according to its registration. Thus, pinpointing the origin of an offending packet is extremely challenging.

d. This handicap is often referred to as the Internet's vulnerability to cyber attacks, namely, DoS (Denial of Service)[26]. Since the attackers create their own spoofed IP addresses, they may appear to originate from any institution whose allocated address block ranges happen to cover the spoofed address. The advanced version, DDoS (Distributed DoS) is even more troublesome, because it utilizes multitudes of compromised systems in unison to attack one target simultaneously. Since the origins of the packets are hard to identify, locating the perpetrator is nearly impossible. Certain

[24] Owner's Installation & Operation Manual, Model: VN100, Page 24, Appendix A.1 a.: http://www.avinta.com/techsupport-1/manuals/vn100manual/vn100om.pdf
[25] BitDefender BOX: http://www.bitdefender.com/box/#overview
[26] Denial of Service Attacks: http://en.wikipedia.org/wiki/Denial-of-service_attack

tools[27] on the Internet may appear to be impressively capable of dealing with this issue, until one realizes that each of the captured IP address (most likely spoofed) points to an unwary ORGANIZATION who owns it. Consequently, the decoded LOCATION is meaningless. In this respect, no literature has indicated that IPv6 could fair better than IPv4[28].

C. Myth 5: IPv6 addressing is not more complicated than IPv4

This statement appears odd. By just looking at the number of bits involved, it is hard to conclude that the 128-bit Hex-decimal formatted IPv6 numbering system would not require more human skill or electronic processing power to handle than the 32-bit dot-decimal IPv4 numbering system. Perhaps this is just referring to the improved header format?[29]

D. Myth 6: IPv6 does not burden IoT

Similarly, the direct exposure to the Internet requiring individualized security measures against intrusion should increase the demand on IoT's processing power while operating with IPv6. Justifications for the contrary have not been located.

E. Myth 7: Internet packet routing vs. PSTN circuit switching

As mentioned in the discussions above, one subtle yet perhaps critical issue surfaced during the study of the above topics. The issue has to do with the philosophy behind the choice of information that should be encoded in the identification of a device intended for public global communication. Logically, the locality is probably the most important one, because it enables the communication system to find the most direct, expedient and efficient route to connect the parties by examining the location information encoded in their respective identifications. Without such information, a connection between two neighbors, in the worst case, might span around the globe.

a. Although the name implies distance, telephone service began with relatively local coverage. It grew beyond regional and national boundaries to finally become a global network, which is today generally referred to as PSTN. In the process, each PSTN subscriber is identified by a number that inherently carries the location information. For example, a North American telephone number[30] is in the form of +1 (NPA) EXC-NMBR, where "1" represents North America Zone including several

---

[27] Live Attack Map: http://map.ipviking.com/

[28] Why the Internet of Things Needs IPv6: http://www.govtech.com/policy-management/Why-the-Internet-of-Things-Needs-IPv6.html -- Page 3/5 -- Interview of Vint Cerf: And like all tech implementations, security is another issue – neither IPv6 nor IPv4 protect against denial of service attacks, for example. "Switching from one protocol to the other or running them both in parallel doesn't solve that problem, which simply means we have many other things to worry about," Cerf said.

[29] IPvX: Better than IPv6?: https://samsclass.info/ipvx/

[30] List of North American Numbering Plan Area Codes: http://en.wikipedia.org/wiki/List_of_North_American_Numbering_Plan_area_codes

countries, such as USA, Canada, etc.[31] "NPA" (Numbering Plan Area) is commonly known as Area Code which usually covers part of a State or a small country[32]. An "EXC" (EXChange) code used to cover a small city or a large town. As they grow, cities or towns may now have one or more EXC codes. In fact, some major city based metropolitan areas now occupy several NPA codes. Regardless of the evolution, the first three parts of a North American telephone number continue to pinpoint the location of a subscriber to be within a fairly confined geographical area. Only the "NMBR" part is randomly assigned. Even so, according to wired telephony practice, a NMBR is affixed to a specific street number in a Telco's records. This encoding scheme enables the CO (Central Office) where a call is originated to look for the best route to the destination party according to the number dialed. With hierarchical routing fabric deployed in the PSTN, this process has been very concise and predictable, even with the strategy of several levels of backup routing. And, tracing back to a caller during emergency situation such as 911 Service is a deterministic process.

b. With the advent of cellular telephone service, it seems that the above principle may not work anymore, especially, the latest practice of granting a mobile phone subscriber the number portability to an area served by another company. It turns out that the roaming functionality, inherent in the cellular phone system operation process, allows not only a mobile phone user to occasionally travel to different service areas, but also to permanently relocate to another part of the world. This is because the home CO always knows the mobile phone's current location by updates from the CO where the mobile phone has signed in. When a mobile phone is not in its home service area, a call to it only requires one extra step of being redirected by the home CO to the current serving CO for handling. Furthermore, if needed, a mobile phone may be located by utilizing radio signal triangulation technique among cellular towers. In short, the PSTN numbering plan enables an edge (Class-5) switching machine with sufficient intelligence to act directly, with the destination (or the re-directed) CO, upon a dialed telephone number in a distributed fashion, without central coordination.

c. The IP address used in the Internet appears to take a different approach. The highest level IPv4 address blocks used to be allocated to institutions such as government, universities, research or large business entities, ISPs, etc. Since each of these institutions may have installations or subscribers anywhere around the globe, this convention essentially creates multiple overlapping worldwide networks. Although cooperative routing strategies have been worked out among them, they just could not be as concise and efficient as those deterministic PSTN processes.

d. The recent trend of consolidating high level IPv4 address block allocations into five RIRs (Regional Internet Registries)[33] may help to streamline the routing process. However, at the next level, the NIRs (National Internet Registries)[34] appear to continue

[31] List of Country Calling Codes: http://en.wikipedia.org/wiki/List_of_country_calling_codes
[32] North American Telephone Area Codes: http://www.convertit.com/Go/ConvertIt/Reference/Telephone_Area_Codes.ASP
[33] Regional Internet Registry: http://en.wikipedia.org/wiki/Regional_Internet_registry
[34] National Internet Registry: http://en.wikipedia.org/wiki/National_Internet_registry

the past practice of allocating IP addresses to institutions and businesses, without further dividing the geographical territories into smaller areas. The net result is still multitude overlapping worldwide networks that require significant coordination to route a packet.

e. While there must be many reasons for the Internet to continue its current format for encoding the IP address, the resulting complexity appears to be in fundamental contradiction to its declared intention of empowering the general public. By contrast, the common perception is that Telcos monopolize telephony services, but telephone numbers, being affixed to geographical areas, have never been controlled or owned by a particular regulated telephone operating company. When the service of an area changes hands, all number assignments remain intact and are assumed by the new Telco. Subscribers are not affected by such business transactions.

f. Since public IP addresses are assigned by an ISP from its own allocated block received from NIR, changing ISP means the affected subscribers need to get new IP address assignments. This issue has not been felt by the general public up to now, because most consumers have been assigned with dynamic IPv4 addresses through ISP's DHCP server. Even though ISPs occasionally reassign these numbers, e. g., after a major power cycling event, no consumer has been paying attention to the actual value of such numbers since most of their devices have never expected being contacted by a remote party, until the recent IoT type of operations.

g. To ensure end-to-end connectivity by addressing IoTs directly, static IPv6 addresses would likely be used, so that a subscriber may give such information out to a friend to enjoy the benefits. This will lead to complications. With each IoT's IP address assigned by the ISP when it is first put in use, it is locked into that ISP's IPv6 address block. What happens if the owner moves to a location served by another ISP? Can each IoT's address be ported to the new residence? Or, if a different ISP moves into a service area, should all IoT addresses in that area be changed? If not, an IoT with IPv6 address may become a hostage of the ISP who initially assigns the IPv6 address to it. On the other hand, if an IoT's IPv6 address is permanent and portable, each and every ISP's worldwide IPv6 address map will soon become fragmented beyond imagination as the result of the general population constantly relocating. This will burden the Internet routers tremendously.

h. The contrast with the limited number of "monopoly" Telcos regulated by respective governments is stark. The Internet is now controlled by many medium to small un-regulated "free" enterprises, each controlling a sizable chunk of IP addresses and exerting its respective business tactics on consumers. Just this diversity is mind-boggling.

8. Summary & Discussion

A. ExIP (Extended IPv4) public address

a. By mimicking a PABX in extending the PSTN numbering plan, a scheme for reclaiming part of the already allocated private network address block 192.168/16 to relieve IPv4 address pool shortage is proposed.

i. Reusing the 192.168.0/24 block behind each public IPv4 address enables the overall publicly identifiable entities to be multiplied by 256 times. This is more than 137 times the projected Year 2020 population of 7.6 billion, which allows Internet far beyond Year 2020 to occupy only $1/16^{th}$ of the original IPv4 address space, releasing the remaining majority $15/16^{th}$ of the address pool as spares.

ii. The last octet of the address block, 192.168.nnn.0/32 offers 256 combinations per entity for the projected need of 6.58 IoTs per person by Year 2020. This even enables each consumer to "randomize" the use of these numbers to enjoy some basic defense against intruders.

iii. This scheme may be implemented by simply enhancing the software in the edge routers to realize the semi-public router function, with no need to modify existing hardware and interconnections.

b. The other driving force for IPv6 is the popularity of mobile devices such as smart phones. This application may be justified because of their mobility worldwide. However, this should not be the reason to wrap all IoTs into the same class, because IoTs are mostly stationary on premises. Such IoTs do not need an individual public identity on the Internet. They should function fine on a private network with the proposed ExIP scheme. On the other hand, since most smart phones have Wi-Fi mode which allows them to log in to a LAN / HAN for Internet access, they may be assigned with temporary private network addresses whenever they come within range of a LAN / HAN that they are authorized to use.

c. Note that since the ExIP scheme is capable of addressing every individual on this planet, whatever IoTs (including mobile phones) that person carries around may be handled as part of a private network within the reusable 192.168.nnn.0/32 address block. Of course, the mobile phone roaming technology needs be replicated in the Internet to support the roaming and portability. That is, upon receiving a session initiating packet with the requesting host address outside of the authorized range, an edge router will first request authentication from the edge router that is responsible for such an address, before allowing the packet to enter Internet.

d. Considering savvy users who may have more than 256 IoTs, the proposed technique may be applied to two other lesser know reserved private business address blocks, 10/8 and 172.16/12 that may multiply each IPv4 public address by 16M and 1M times, respectively. An overall migration plan to ExIP (Extended IPv4) for not only relieving IPv4 address shortage immediately, but also satisfying the long term usage has been proposed in this paper.

B. IPv6 / CENTREX vs. IPv4 + NAT & DMZ / PABX

A fairly concise analogy has been established between the Internet and PSTN components and operation. That is, IPv6 is like CENTREX while IPv4 with semi-public routing supported by NAT and DMZ is like PABX. The former pair allows direct connection through a public communication system with faster setup time, but lacks a baseline of defense against intrusion. The latter pair may be a bit slower in establishing a connection, but has a simple first line of defense against hackers. In addition, IPsec that applies to both IPv6 and IPv4 payloads, is equivalent to audio scrambling technologies that apply to voice traffic through CENTREX and PABX. In fact, both are measures mostly implemented in the communicating end devices.

C. Encoding the device identifier

There seems to be a philosophical disagreement about what information should be carried in the address of a device that communicates through a global public network. Logically, the more specifically the address is associated with the physical coordinates of a device's locality, the easier it is to accomplish the routing tasks during operation. The current practice of allocating blocks of addresses for businesses like ISPs to assign to end users may be counter productive to the goal of Internet. This is because the IoTs are then not only devoid of location identification, but also locked to a specific ISP, making portability between either locations or ISPs difficult. In this respect, IP addresses (both v4 and v6) seem to resemble the MAC (Media Access Control)[35] address assigned to a NIC (Network Interface Controller) that communicates over Ethernet (wired or wireless). MAC addresses begin with an OUI (Organizationally Unique Identifier) that is allocated to a manufacturing organization. Since Ethernet was originally designed for LAN, locality is known and fixed and there is no need to encode it into the device identification. The first important level of tag would be the OUI to facilitate troubleshooting. This kind of header does not seem to be warranted for IoTs, because the current location of an IoT should be much more important than who made the device, or is in charge of the IP address in question.

D. Network robustness

In terms of performance, a large, especially global, system's robustness probably is just as important as the service it provides because the diagnosis, repair and recovery efforts are monumental when its operation is disrupted. In this regard, it is surprising that the frequent hacking of the Internet has come to be accepted as inevitable in light of its inherent characteristics. The most notable example is the recent compromising of Sony Picture Entertainment's computer system. Damages aside, it appears that merely tracking down the perpetrator to a specific country is such a huge job that it is beyond the capability of security professionals, but requires the involvement of the FBI (Federal Bureau of Investigation)[36]. Could this be the consequence of IoT's IP addresses carrying no geographical information and the extensive use of DHCP by ISPs? If geographical location information is encoded in the IP address format and practiced in the operation,

[35] MAC Address: http://en.wikipedia.org/wiki/MAC_address
[36] FBI confirms North Korea behind Sony hack:
http://www.usatoday.com/story/news/2014/12/19/sony-the-interview-hackers-gop/20635449/

the governing edge router would immediately spot a spoofed address and prevent the packet from entering the Internet, since it does not belong to that router's jurisdiction. Then, tracking down the violator becomes a finite task. It is significant to note that no one seems to have taken advantage of this high-profile hacking event to promote IPv6.

Internet hacking has a close analogy to un-wanted call precedent in PSTN as described in the Appendix. The un-wanted call issue has been mostly resolved via technical means. Unfortunately, latest business practice of allowing telemarketing machine to spoof its Caller-ID information is enabling it to persist. This is a perfect mirror for illustrating why the sources of offending Internet packets are so hard to trace.

E. Divide and Conquer

Last but not least is another subtle yet critical philosophical issue that was uncovered during the above study. As is common knowledge, "a chain is only as strong as its weakest link". To properly manage a large system, the first rule is to utilize the "Divide and conquer" principle to break down a system into subsystems. This facilitates the troubleshooting process of isolating a problem by allowing a division of responsibility for the parallel investigation of the separate subsystems.

a. The most natural place to establish this division, as practiced by the four traditional utilities, water, gas, electricity and telephony, is at the demarcation line where public services enter a subscriber's private premises. This enables the utility to stop a water or gas leak, for example, at the subscriber's meter, instead of affecting an entire neighborhood or even beyond. Similarly, when there is an electricity issue, the circuit breaker at the meter is the first thing that the electric company will shut off if it had not already been tripped. The CPE (Customer Premises Equipment)[37] defined and certified by FCC Part 68[38] is accredited for the fast growth of telephony CPE business. It seems logical, as much in the literature frequently seems to imply, that IoTs on private networks should fall into the category of FCC-defined CPEs, that are not part of the Internet.

b. For global broadband communication, the most important task should be to protect the integrity of a network by isolating it from connected IoTs. What happens to an IoT on a customer premises is its owner's business, unless an outsider is invited to assist. The current push for IPv6 end-to-end connectivity such that all on-premises IoTs are directly addressable from Internet defeats this basic discipline of respecting the individual's privacy. At the same time, it greatly complicates the task of troubleshooting the Internet by virtue of the huge number of IoTs attached, not to mention the creation of an open path for the hackers to exploit the vulnerability of IoTs around every private residence.

c. When the Internet was in its infancy, all host devices were handled by friendly and technically savvy participants and it was reasonable to view the Internet as an end-to-end system. Nowadays, however, IoTs are made by so many different vendors,

[37] Customer-Premises Equipment: http://en.wikipedia.org/wiki/Customer-premises_equipment
[38] Title 47 CFR Part 68: http://en.wikipedia.org/wiki/Customer-premises_equipment

and used by enormous numbers of technically uninitiated, if not hostile, consumers that the end-to-end perspective may no longer be appropriate.

d. As touched at various points throughout our report, Internet is actually much harder than PSTN to deal with from the public interest point of view. The former is a collection of rather disorganized parties, encouraging individualized contributions. As such, however, it is very difficult for any outsider to know enough to be able to critique the inner workings. Since Internet's current overall performances are far from convincing, the long term prospects of letting such a "system" to replace PSTN is very scary, to say the least. We need to act collectively to iron out all the hidden twists for the sake of the general public, if not the national security.

F. Root Cause vs. Manifestations

In closing, we believe that taking a hard look beneath the many symptomatic problems of the Internet in order to get to their root causes is what is required at this stage of its development. We also strongly believe that lessons learned from over a century of experience in PSTN can be gainfully applied to assist in laying the foundation for a robust Internet.

Appendix Precedence & Parallelism

A. Precedence

Telephone service may appear to a layman as nothing more than a telephone set plugged into a wall jack. In fact, there are many behind-the-scene facilities and mechanisms that deal with a wide range of operational requirements which make telephony so reliable and simple to use.

a. To improve on-site switching efficiency among subscribers situated within the proximity of an institution, such as a government office, business, hospital, hotel, etc., PBX (Private Branch eXchange)[39] technology was developed. One of its benefits is that its traffic concentration capability relieves the demand on the PSTN telephone number pool. That is, fewer public telephone numbers are needed for such a group of subscribers to communicate with the rest of the world.

b. Although PBX equipment was originally designed to be located on a subscriber's premises, it may be co-located in the Telco's CO to allow CO staff to manage it. Sometimes the physical equipment of a co-located PBX can even be part of the CO's local (Class-5) switching machine that is loaded with enhanced operation software.

c. Co-located PBX is often confused with another business class telephone service called CENTREX (CENTRal office EXchange)[40], due to very similar operational characteristics. One definitive differentiation between the two is the numbering plan. Each CENTREX station occupies a PSTN number. Consequently, a CENTREX station may be reached directly by just dialing its PSTN number. On the other hand, a PBX station is reached by first dialing the PSTN number representing the institution, followed by specifying the Extension number assigned to it by the institution owner. The last step used to be handled by human attendants (operators or receptionists). With the advent of electronic AA (Auto-Attendant), the calling party may dial the desired Extension number upon hearing the greeting message from the AA. PBX equipped with AA is thus referred to as PABX (Private Automatic Branch eXchange).

d. The extra call setup step to reach a PBX station may be regarded as a rudimental security measure, because it offers a simple screening mechanism against intrusion from an un-wanted caller who does not know the Extension number. Note that CENTREX can not provide this level of defense, because each station is directly accessible from any other subscriber on the PSTN via the public telephone number.

[39] Business Telephone System: http://en.wikipedia.org/wiki/Business_telephone_system
[40] CENTREX: http://en.wikipedia.org/wiki/Centrex

e. This extra setup step in PBX does impose additional time delay in establishing a call. However, this drawback may be circumvented by implementing a procedure utilizing Caller-ID (Caller-IDentification) technology[41]. Essentially, with proper Caller-ID facility in PSTN and terminating PABX, it is possible for a caller to establish a call to a desired PABX station directly as if it were on the public network, by simply appending the initial dialing string with a few more key strokes representing the desired Extension number at the destination. Note that the original PBX defense mechanism against un-wanted callers is not affected by this enhancement.

f. Although the AA capability in PABX can block un-wanted callers, a persistent telemarketer can be rather annoying. In fact, the extreme cases can even get to the point of blocking the normal use of the telephone services (the telephony equivalent of Denial of Service). The natural counter measure is to utilize the Caller-ID facility for tracing back to the perpetrator. This turns out to be no more as straightforward as it used to be, because nowadays such information is often manipulated by the calling party. Spoofed Caller-ID may appear to a naked eye as being meaningless, frequently done by high end telemarketer calling machines that the serving Telcos apparently have granted such capability as part of the "marketing tool"[42]. Yet, when necessary, the caller may still be promptly identified by the actual calling number and the trunks utilized between switching machines in setting up the circuit for such a call. This is because such information is recorded as part of the billing system, called CAMA (Centralized Automatic Message Accounting)[43], to validate the charge. However, this is such a highly involved technical topic, hardly anyone is aware of it, let alone being requested by an irritated consumer.

g. Another behind-the-scene PABX technology that further reduces the demand for PSTN public phone numbers is that each PBX actually needs only one PSTN number, even for a very large institution. This is made possible because of the ACD (Automatic Call Distribution)[44] capability of CO switching machines. On the PBX side, the multiple voice channels for accessing PSTN simultaneously by several office workers are carried by a corresponding number of "PBX trunks" to CO. The same are called in CO terminology as "subscriber lines", because each is basically the same as the loop serving a residential home. Each PBX Trunk is supported by a corresponding "port" on the CO's SLIC (Subscriber Line Interface Circuit) equipment.

h. Lastly, although seldom utilized by ordinary telephone users, privacy of communication can be ensured by encrypting the voice payload of a call at the speaker end and then decrypting it at the listener end by means of an equipment pair owned by subscribers on either end of a call.

---

[41] Extended Public Switched Telephone Network Architecture with Enhanced Subscriber Control on Call Setup: US Patent No. 5,930,346.
[42] Caller ID Spoofing: http://en.wikipedia.org/wiki/Caller_ID
[43] Automatic message accounting: http://en.wikipedia.org/wiki/Automatic_message_accounting
[44] Automatic Call Distributor: http://en.wikipedia.org/wiki/Automatic_call_distributor

B. Parallelism

In this section, we will describe the close resemblance between Internet-router relationship and PSTN switching system architecture. In particular, the proposed semi-public router for extending Internet addressing capability may be viewed as serving the same function as that provided by PABX to extend the PSTN numbering plan.

a. As a specific example, the telephony infrastructure can be used to implement the semi-public (192.168.0/24) routers which may be treated as secondary DSLAM (Digital Subscriber Line Access Multiplexer)[45] modules that could be housed in the loop plant B-Boxes[46] that are distributed in the neighborhood near subscribers. This is very much like the basic PABX.

b. Next, these secondary DSLAMs may be co-located with the primary DSLAMs currently residing in the CO, because the individual subscriber copper pairs originate from here. This is very much the same as the CO co-located PABX, or CENTREX.

c. On the other hand, where FTTN (Fiber To The Neighborhood) technology has been deployed, the primary DSLAMs have been moved out to the neighborhood B-Boxes anyway. For such cases, the merging of primary and secondary DSLAMs will then occur in the B-Box. This configuration is very much the same as Telco's VoIP (Voice over Internet Protocol)[47] capability for updating the traditional POTS (Plain Old Telephone Service)[48].

d. The DMZ-bypassing NAT function allowing un-invited inbound session requesting packet to reach a desired destination is very much the same as the AA capability on a PABX that enables a caller to specify an extension number for direct connection through one extra stage of switching process. Note that in either case, as soon as the desired destination party responds to the initial connect request, the actual communication session is not affected by either DMZ or AA subsystems, respectively.

e. Similar configurations would apply to Internet service deliveries deployed over cable, fiber, satellite, etc. Implementation details for these are beyond the scope of this paper.

f. The current practice of assigning IP addresses to various devices to share one private data network is very much the same as using additional telephony station sets, external ringers, cordless phones, TADs (Telephone Answering Devices), MODEMs (MOdulator DEModulators), FAX (FACSimile) machines, Caller-ID detectors, etc. to share one voice telephone line. The difference is that the latter were developed through a

---

[45] Digital Subscriber Line Access Multiplexer: http://en.wikipedia.org/wiki/Digital_subscriber_line_access_multiplexer
[46] Privateline.com: Outside Plant, B-Boxes: http://www.privateline.com/OSP/No.html
[47] Voice over IP: http://en.wikipedia.org/wiki/Voice_over_IP
[48] POTS:: http://en.wikipedia.org/wiki/POTS

series of efforts spread over a long period of time. Instead of using explicit addresses or identification numbers for each device, the interactions between them, or protocols, were worked out as each new type of device emerge and embedded in their respective operation characteristics. Nevertheless, there are certain interaction protocols that users must pay some attention to. Utilizing dPABX technology, each of these devices may now be assigned with a unique extension number. Consequently, they may be operated as if they were on separate telephone lines.

g. The port number assigned to different sessions by the NAT in an RG is equivalent to the CO's SLIC Port for interfacing with PBX trunk. One recent IPv4 development furthers this by utilizing the Address Plus Port (A+P) technique to expand the addressing capability[49].The difference is that for the PABX case, the trunks are dynamically shared among users as needed. For the A+P case, the port is intended to be a permanent assignment to individual IoTs. In addition, the A+P approach will require the upgrade of RGs or IoTs to be aware of the new A+P convention.

h. The proposed porting of IPv4 address allocations to a group of reserved address blocks to free up the larger currently used blocks is very much analogous to the telephony practice of having a spare tube in an underground conduit run. It enables a new cable to be pulled through for taking over the traffic in a degraded old one. If the new cable is much more capable, such as an optical fiber, it will consolidate several existing copper-pair cables, creating even more spare tubes for other capabilities in the future.

i. One historical telephony technology deserves to be mentioned here for reference. The US military used to have a worldwide voice communication network, called AUTOVON (AUTOmatic VOice Network) [50] that mostly resembled PSTN, since it was developed and maintained by AT&T. AUTOVON's own set of numbering plan was similar to the North American Numbering Plan. The major features of AUTOVON were 4-wire connection[51] throughout and preempt authority by higher ranking officers. At various points, AUTOVON was interconnected with the PSTN facility, primarily for transmission backup redundancy. Thus, the AUTOVON in worldwide telephony is very much analogous to one IP address block allocated to an operational institution in the Internet. As a matter of fact, over half a dozen highest level IPv4 address blocks, such as 006/8, 011/8, 022/8, 026/8, 029/8, 030/8, 055/8, 214/8, 215/8, etc. are allocated to US-DoD related agencies[52]. Each of these may be viewed as a digital version of the AUTOVON operating in parallel with the civilian Internet.

[49] Address plus Port: https://en.wikipedia.org/wiki/Address_plus_Port
[50] AUTOVON: http://en.wikipedia.org/wiki/Autovon
[51] Four-Wire Circuit: http://en.wikipedia.org/wiki/Four-wire_circuit
[52] US-DoD IPv4 Address Blocks: http://www.iana.org/assignments/ipv4-address-space/ipv4-address-space.xhtml

Glossary

A+P:	Address Plus Port – IETF RFC6346
AA:	Auto-Attendant
ACD:	Automatic Call Distribution
AT&T:	American Telephone & Telegraph Corporation
AUTOVON:	AUTOmatic VOice Network
B-Box:	Telephone loop plant service access junction cabinet usually located within one mile or so from subscriber cluster
Caller-ID:	Caller-IDentification
CAMA:	Centralized Automatic Message Accounting
CENTREX:	CENTRal office EXchange
CO:	telephone Central Office
CPE:	Customer Premises Equipment
Demarcation:	A conceptual responsibility separation line between a public utility and a customer / subscriber
DHCP:	Dynamic Host Configuration Protocol
DMZ:	De-Militarized Zone
DoD:	Department of Defense
DDoS:	Distributed DoS
DoS:	Denial of Service
dPABX:	distributed PABX
DSLAM:	Digital Subscriber Line Access Multiplexer
EnIP:	Enhanced IPv4 addressing technique (http://www.enhancedip.org/)
ExIP:	Extended IPv4 addressing technique (proposed by this paper)
EXC:	EXChange
FAX:	Facsimile
FCC:	Federal Communications Commission
FBI:	Federal Bureau of Investigation
FTTN:	Fiber To The Neighborhood
HAN:	Home Area Network
IANA:	Internet Assigned Numbers Authority
IETF:	Internet Engineering Task Force
IoT:	Internet of Thing
IPsec:	IP SECurity
IPv4:	Internet Protocol version 4
IPv6:	Internet Protocol version 6
ISP:	Internet Service Provider
LAN:	Local Area Network
MAC:	Media Access Control
MODEM:	MOdulator-DEModulator
NAT:	Network Address Translation
NIC:	Network Interface Controller
NIR:	National Internet Registry

NMBR:	telephone NuMBeR
NPA:	Numbering Plan Area (commonly known as Area Code)
NSA:	National Security Agency
OUI:	Organizationally Unique Identifier
PABX:	Private Automatic Branch eXchange
PBX:	Private Branch eXchange
Port Number:	A session identification number assigned by NAT for sharing the same IP address
POTS:	Plain Old Telephone Service
PSTN:	Public Switched Telephone Network
RFC:	Request For Comments
RG:	Residential Gateway
RIR:	Regional Internet Registry
SLIC:	Subscriber Line Interface Circuit
TAD:	Telephone Answering Device (such as answering machine)
Telco:	TELephone COmpany
TOR:	The Onion Router
VoIP:	Voice over Internet Protocol