<Network Working Group>
Internet Draft
Intended status: Experimental
Expires: December 2025

A. Y. Chen
R. R. Ati
Avinta Communications, Inc.
A. Karandikar
India Institute of Technology
D. R. Crowe
Wireless Telcom Consultant

June 25, 2025

Adaptive IPv4 Address Space
draft-chen-ati-adaptive-ipv4-address-space-18.txt

Abstract

This document describes a solution to the Internet address depletion issue through the use of an existing Option mechanism that is part of the original IPv4 protocol. This proposal, named EzIP (phonetic for Easy IPv4), outlines the IPv4 public address pool expansion and the Internet system architecture enhancement considerations. EzIP may expand an IPv4 address by a factor of 256M without affecting the existing IPv4 based Internet, or the current private networks. It is in full conformance with the IPv4 protocol, and supports not only both direct and private network connectivity, but also their interoperability. EzIP deployments may coexist with existing Internet traffic and IoTs (Internet of Things) operations without perturbing their setups, while offering end-users the freedom to independently choose which service. EzIP may be implemented as a software or firmware enhancement to Internet edge routers or private network routing gateways, wherever needed, or simply installed as an inline adjunct hardware module between the two, enabling a seamless introduction. The 256M case detailed here establishes a complete spherical layer of an overlay of routers for interfacing between the Internet fabric (core plus edge routers) and the end user premises or IoTs. Incorporating caching proxy technology in the gateway, a fairly large geographical region may enjoy address expansion based on as few as one ordinary IPv4 public address utilizing IP packets with degenerated EzIP header. If IPv4 public pool allocations were reorganized, the assignable pool could be multiplied 512M fold or even more. Enabling hierarchical address architecture which facilitates both hierarchical and mesh routing, EzIP can provide nearly the same order of magnitude of address pool resources as IPv6 while streamlining the administrative aspects of it. The basic EzIP will immediately resolve the local IPv4 address shortage, while being transparent to the rest of the Internet as a new parallel facility. Under the Dual-Stack environment, these proposed interim facilities will relieve the IPv4 address shortage issue, while

affording IPv6 more time to reach maturity for providing the availability levels required for delivering a long-term general service. The basic EzIP may be deployed in two distinctive phases. First, the CG-NAT operation may be enhanced by enabling the use of 240/4 netblock in addition to the current 100.64/10 netblock of RFC6598. This makes end-to-end connectivity feasible within the service area of each 240/4 netblock. Second, this capability may extend to global coverage with the use of the Option Word mechanism in the IP header.

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt

The list of Internet-Draft Shadow Directories can be accessed at https://www.ietf.org/shadow.html

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on December 25, 2025.

Copyright Notice

Table of Contents

1. Introduction.....5
1.1. Contents of this Draft.....6
2. EzIP Overview.....7
2.1. EzIP Numbering Plan.....7
2.2. Analogy with NAT.....9
2.3. EzIP System Architecture.....10
2.4. IP Header with Option Word.....12
2.5. Examples of Option Mechanism.....13
2.6. EzIP Header.....14
2.7. EzIP Operation.....15
3. EzIP Deployment Strategy.....15
4. Updating Servers to Support EzIP.....18
5. EzIP Enhancement and Application.....19
6. Security Considerations.....23
7. IANA Considerations.....23
8. Conclusions.....23
9. References.....24
9.1. Normative References.....24
9.2. Informative References.....24
10. Acknowledgments.....25
Appendix A. EzIP Operation.....26
A.1. Connection between EzIP-unaware IoTs.....26
A.1.1. T1a Initiates a Session Request towards T4a.....26
A.1.2. RG1 Forwards the Packet to SPR1.....27
A.1.3. SPR1 Sends the Packet to SPR4 through the Internet..28
A.1.4. SPR4 Sends the Packet to T4a.....29
A.1.5. T4a Replies to SPR4.....30
A.1.6. SPR4 Sends the Packet to SPR1 through the Internet..31
A.1.7. SPR1 Sends the Packet to RG1.....32
A.1.8. RG1 Forwards the Packet to T1a.....33
A.1.9. T1a Sends a Follow-up Packet to RG1.....33
A.2. Connection Between EzIP-capable IoTs.....34
A.2.1. T1z Initiates a Session Request towards T4z.....34
A.2.2. RG1 Forwards the Packet to SPR1.....35
A.2.3. SPR1 Sends the Packet to SPR4 through the Internet..36
A.2.4. SPR4 Sends the Packet to T4z.....37
A.2.5. T4z Replies to SPR4.....38
A.2.6. SPR4 Sends the Packet to SPR1 through the Internet..39
A.2.7. SPR1 Sends the Packet to RG1.....40
A.2.8. RG1 Forwards the Packet to T1z.....41
A.2.9. T1z Sends a Follow-up Packet to RG1.....42
A.3. Connection Between EzIP-unaware and EzIP-capable IoTs....43
A.3.1. T1a Initiates a Request to T4z.....43
A.3.2. T1z Initiates a Request to T4a.....43

Appendix B. Internet Transition Considerations....44
B.1. EzIP Implementation....44
B.1.1. Introductory Phase....44
B.1.2. New IoT Operation Modes....45
B.1.3. End-to-End Operation....45
B.2. SPR Operation Logic....45
B.2.1. Sending an IP packet out for an IoT or an RG....46
B.2.2. Receiving an IP packet from the ER....46
B.3. RG Enhancement....46
B.3.1. Initiating Session request for an IoT....46
B.3.2. Receiving a packet from the SPR....46
Appendix C. EzIP Realizability....48
C.1. 240/4 Netblock Capable IoTs....48
C.2. 240/4 Netblock Capable Routers....48
C.3. Enhancing an RG....49
C.4. SPR Reference Design....50
C.5. RAN Deployment Model....50
C.5.1. Root / Gateway SPR:....50
C.5.2. Intermediate SPRs:....51
C.5.3. RG SPR:....51
Appendix D. Enhancement of a Commercial RG....52
D.1. Candidate Code for Modification....52
D.2. Proposed Modification....53
D.3. Performance Verification....53
Appendix E. Utilizing Open-Source Router Code....54
E.1. EzIP Realizability Test Bed....54
E.2. RAN Architecture Demonstration....54
E.3. EzIP Compatible Routers....55
Appendix F. Sub-Internet....56
F.1. Gateway Configuration....56
F.2. Gateway Setup....56
F.3. Sub-Internet Operation....56
Appendix G. Discussions....57
G.1. Activation of EzIP Capability....57
G.2. EzIP Network Architecture....57
G.3. EzIP Deployment Vehicles....58
G.4. 240/4 Address Administration....59
G.5. Routing Strategy....59
G.6. Network Robustness....60
G.7. Cost....60
G.8. Redundancy....60
Appendix H. Manifestations and Implications....61
Appendix I. Miscellaneous Considerations....63
Appendix J. Streamline The Internet....67
J.1. Enhancing the existing facility....67
J.2. Address administration....68
J.3. Intra-RAN networking and routing....69

J.4. Communication beyond a RAN.....69
J.5. Deployment sequence.....69
Appendix K. A More Robust Internet.....71
K.1. A Decentralized Internet.....71
K.2. A Deterministic Internet.....71
K.3. A Secure Internet.....72

1. Introduction

For various reasons, there is a large demand for IP addresses. It would be useful to have a unique address for each Internet device, such that, if desired, any device may call upon any other directly. IP addresses are needed while client devices, such as mobile phones, are attached to the internet, which is a rapidly increasing demand. The Internet of Things (IoT) would also be able to make use of more routable addresses if they were available. Currently, these are not possible with the existing IPv4 configuration.

By Year 2020, the world population and number of IoTs are expected to reach 7.6B (Billion) and 50B respectively, according to a 2011 Cisco online white paper [3]. Note that the world population is now over 8B. On the other hand, the IoTs deployed appears to much fewer than predicted. However, the exact numbers do not affect the analysis in this document.

The IPv4 dot-decimal address format, consisting of four octets each made of 8 binary bits, provides a little over 4 billion unique addresses (256 x 256 x 256 x 256 equals 4,294,967,296 - decimal exact). Using the binary / shorthand 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 (Million), or 4.096B (or, further rounded down to 4B for quick estimate calculations). Clearly, the predicted demand is more than 12 times over the inherent capacity available from the supply.

IPv6, with its 128-bit hexadecimal address format, is four times as long as the IPv4, has 256BBBB (4B x 4B x 4B x 4B) unique addresses. It offers a promising solution to the address shortage. However, its global adoption appears to be facing significant challenges [4], [5].

Interim relief to the IPv4 address shortage has been provided by Network Address and Port Translation (NAPT - commonly known simply as NAT) on private networks together with Carrier Grade NAT (CG-NAT or abbreviated further to CGN) [RFC6598] [6] over the public Internet. However, NAT modules slow down routers due to the state-table look-up process. As well, they only allow an Internet session

be initiated by their own clients, impeding the end-to-end setup requests initiated from remote devices that a fully-fledged communication system should be capable of. Since port numbers are used to effectively increase the size of the address pool, they introduce complex and suboptimal port management requirements. For example, being dynamic, the state-table used by CG-NAT increases Cyber Security vulnerability by imposing extra efforts to forensic tracing of perpetrators. On the other hand, private network NAT as part of a Routing / Residential Gateway (RG) does provide a rudimentary defense against intrusion. To minimize the confusion, we will explicitly label this latter (although implemented first) NAT as RG-NAT in this document to distinguish from the CG-NAT.

If IPv4 capacity could be expanded without the CG-NAT limitations, such as size, speed and outgoing-only, the urgency due to address shortage will be relaxed long enough for the IPv6 to mature on its own pace.

There have been several proposals to increase the effective Internet public address pool in the past. They all introduced new techniques or protocols that ran into certain handicaps or compatibility issues, preventing a smooth transition.

EzIP utilizes a long-reserved network address block (netblock) 240/4 [7] that all of the existing Internet Core (/ backbone) Router (CR), Edge Router (ER) and private network Routing (/ Residential) Gateway (RG) as well as terminal hosts such as PCs and IoTs are not allowed to utilize. The Option mechanism defined in [RFC791] [1] is used for transporting such information as the IP header payload so that an IP packet is transparent to all of these routers, except a newly defined category named Semi-Public Router (SPR). By inserting an SPR between an ER and a private premises that it serves, each publicly assignable IPv4 address can be expanded 256M fold.

EzIP introduces minimal perturbation by being compatible to the current Internet system architecture. Its deployment will start with an SPR providing public CG-NAT functions to unload the burden from the current CG-NAT facility. With the basic routing as an integral part of the SPR, directly connected individual IoTs and private networks will be encouraged to migrate toward the full EzIP service for enjoying the end-to-end connectivity between and among them.

1.1. Contents of this Draft

This draft outlines the EzIP numbering plan. An enhanced IP header, called EzIP header, is introduced to carry the EzIP address as payload using the Option word. How the Internet architecture will

change as the result of being extended by the EzIP scheme is explained. How the EzIP header flows through various routers, and Internet update considerations are described, with details presented in Appendices A and B, respectively. Utilizing the EzIP approach, several ways to expand the publicly assignable IPv4 address pool, as well as enhance Internet operations are then discussed. Appendix C outlines the experimental effort to demonstrate the feasibility of EzIP by configuring a regional area network model based on current networking equipment upon finite enhancements. Appendix D is a Work-In-Progress report about the enhancement of a specific commercial RG. Appendix E is an EzIP scheme feasibility demonstration by utilizing publicly available hardware and software. Appendix F describes a networking configuration called Sub-Internet that is based on one single IPv4 address. A sub-Internet is a self-contained overlaying network module that can provide Internet-like services to a stand-alone region with up to 256M IoTs or private premises. To facilitate discussing various aspects of this proposal, Appendix G outlines several topics that EzIP may relate to. Appendix H lists a few more manifestations that EzIP proposal may imply. Appendix I distills the EzIP proposal to a more concise perspective for avoiding distractions. Appendix J outlines considerations for streamlining the Internet by deploying the EzIP over the existing CG-NAT facility. Utilizing static addresses, EzIP operations are more deterministic for establishing a robust infrastructure for improved cyber security. Appendix K summarizes the possible EzIP contribution to a couple current Internet topics.

2. EzIP Overview

2.1. EzIP Numbering Plan

EzIP uses the reserved private network address pools in very much the same way that Private Automatic Branch eXchange (PABX) switching machines utilize locally assigned "extension numbers" to expand the Public Switched Telephone Network (PSTN) capacity, by replicating a public telephone line to multitudes of reusable private telephone numbers, each to identify a local instrument, such as telephone, FAX, TAD (Telephone Answering Device), alarm, utility meter reading, etc.

At the first sight, this correlation may seem odd, because the PABX extension numbers belong to a reusable private set separate from that of the public telephone numbers and both are independently expandable, while private network IP address is a specific subset parsed from the overall IPv4 pool that is otherwise all public and finite. However, the fact that neither of the latter two is allowed to operate in the other’s domain, the same as in the telephony

practice, suggests that the proposed EzIP numbering plan indeed may mirror the PABX. For example, extension 123 or 1234 may exist in thousands of different PABX switches without ambiguity. Similarly, the IPv4 private network address blocks (10/8, 172.16/12 and 192.168/16) may also be re-used in many networks without ambiguity.

The key EzIP concept is the partitioning of a finite public address pool to put aside a block of special (called "Semi-Public" in the presentation below) addresses that extends each remaining public address to multitudes of sub-addresses, resulting in an effectively much larger assignable public address resource.

In fact, the initial EzIP analysis identified the untold two-stage subnetting process of 192.168/16 that has been practiced routinely for a long time. End-users are commonly accustomed to an RG choosing one out of 256 values from the fourth octet of the 192.168.K/24 address block for identifying an IoT on a private premises. They mostly are, however, unaware of the preceding stage of selecting the value "K" from the third octet of the 192.168/16 block, as the factory default RG identification assigned by a manufacturer, is implicitly capable of expanding it by 256-fold for supporting a corresponding number of private premises. A key EzIP concept is to use the elusive IPv4 240/4 netblock (240/8 - 255/8), that has been "RESERVED" for "Future use" since 1981-09, as the result of the historical address assignment evolution. It was proposed to be redesignated to "Private Use" over a decade ago [2]. However, as pointed out by its own authors in Section 2, Caveats of Use, "Many implementations of the TCP/IP protocol stack have the 240.0.0.0/4 address block marked as experimental, and prevent the host from forwarding IP packets with addresses drawn from this address block." That proposal did not get advanced. Consequently, to this date, the 240/4 netblock remains practically unused.

Substituting the function of the third octet of 192.168.K/24 with addresses from the 240/4 netblock in the first stage RG and redefining it as a new category of router, called SPR, the EzIP scheme circumvents the earlier hurdles to achieve the address multiplication factor of 256M without involving any existing router. This is because the 240/4 addresses are only used by the SPR and within the Option word header extension. They are not recognized as IPv4 addresses anywhere within the current Internet, while the Option word mechanism can carry them through the network as part of the IP header payload.

Since the 240/4 netblock cannot be used by existing routers, the size of the maximum assignable public IPv4 pool has actually been only 3.84B (4.096B - 256M). So, the overall assignable pool resulted

from the EzIP approach is about 983MB (3.84B x 256M), which is over 19M times of the expected Year 2020 IoTs. This size certainly has the potential to support the short- to mid-term public IP address needs.

2.2. Analogy with NAT

NAT generally works by temporarily assigning a port number to outgoing communications originated from a local / private address, by converting it into a public IPv4 address shared with other local IoTs for external transmission. When responses are received, the port number is converted back into the local / private IPv4 address.

EzIP possesses similarities to CG-NAT, but also has some important differences.

There are a number of limitations of NAT that are not present with EzIP. (1) There are only 65,536 port numbers but 256M 240/4 EzIP addresses; (2) Due to the limited number of ports, assignments are only temporary and will be reclaimed after a period of inactivity, but there are so many EzIP addresses that assignments will be made permanent; (3) Port numbers are used for other purposes than NAT, further reducing the pool, but EzIP uses 240/4 addresses solely for one purpose; (4) Due to the limited time during which a port number is assigned, the NAT port numbers cannot be used for incoming communications, but the EzIP address assignments will be long term and can be used for direct communications between EzIP-aware devices. (5) Intriguingly, while RG-NAT provides rudimental defense against intrusion, the dynamic nature of CG-NAT opens up the Internet vulnerability to cyber-attacks, due to its inherent lack of forensic traceability. SPR could eventually replace CG-NAT for a more efficient and robust path.

2.3. EzIP System Architecture

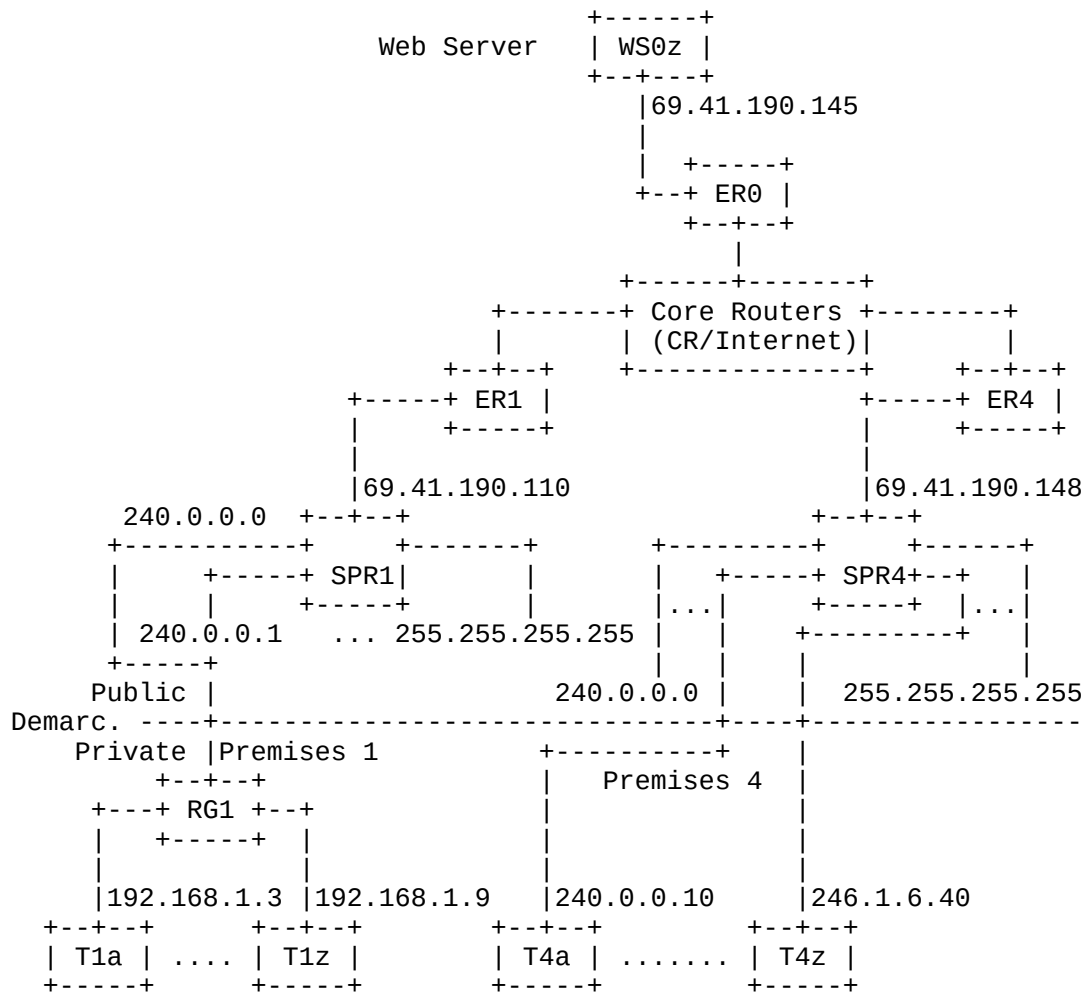

Figure 1 EzIP System Architecture

The new category of router, SPR is to be positioned inline between an ER and the customer premises that it serves. After the original path is re-established, the remaining addresses in the 240/4 netblock will be used by the SPR to serve additional premises. Figure 1 shows a general view of the enhanced Internet system

architecture with two SPRs, SPR1 and SPR4, deployed. Note that the "69.41.190.x" are static addresses. In particular, the "69.41.190.145" is the permanent public Internet address assigned to Avinta.com.

2.3.1. Referring to the lefthand portion labeled "Premises 1" of Figure 1, instead of assigning each premises a public IPv4 address as in the current practice, an SPR like SPR1, is inserted between an ER (ER1) and its connections to private network Routing Gateways like RG1, for utilizing 240.0.0.0 through 255.255.255.255 of the 240/4 netblock to identify respective premises. The RG1, serving either a business LAN (Local Area Network) or a residential HAN (Home Area Network), uses addresses from one of the three private network [RFC1918] [8] blocks, 10/8, 172.16/12 and 192.168/16, such as 192.168.1.3 and 192.168.1.9 to identify the IoTs, T1a and T1z, respectively.

2.3.2. Part of the righthand portion of Figure 1 is labeled "Premises 4". Here SPR4 directly assigns addresses 240.0.0.10 and 246.1.6.40 from the 240/4 netblock to T4a and T4z, respectively. Consequently, these IoTs are accessible through SPR4 from any other IoT in the Internet.

2.3.3. Since the existing physical connections to subscriber’s premises terminate at the ER, it would be natural to have SPRs collocated with their ER for streamlining the interconnections. It follows that the simple routing function provided by the new SPR modules may be absorbed into the ER through a straightforward operational firmware enhancement. Consequently, the public / private demarcation (Demarc.) line will remain at the RG where currently all utility services enter a subscriber’s premises.

2.3.4. To fully tag each of these devices, we may use a concatenated three-part address notation: "Public - Semi-Public: TCP Port". The following is how each of the IoTs in Figure 1 may be uniquely identified in the Internet.

RG1: 69.41.190.110-240.0.0.0

T1a: 69.41.190.110-240.0.0.0:3

T1z: 69.41.190.110-240.0.0.0:9

T4a: 69.41.190.148-240.0.0.10

T4z: 69.41.190.148-246.1.6.40

Note that to simplify the presentation, it is assumed at this juncture that the conventional TCP (Transmission Control Protocol) [RFC793] [9] Port Number, normally assigned to T1a and T1z by RG1's RG-NAT module upon initiating a session, equals to the fourth octet of that IoT's private IP address that is assigned by the RG1's DHCP (Dynamic Host Configuration Protocol) [RFC2123] [10] subsystem as ":3" and ":9", respectively. Such numbers are unique within each respective /24 private network such as the 192.168.1/24 here. They are adequate for the discussion purpose in this document. However, considering security, as well as allowing each IoT to have multiple simultaneous sessions, etc., this direct and singular correlation shall be avoided in actual practice by following the RG-NAT operation conventions as depicted by the examples in Appendix A.

Figure 2 groups IoTs, routers and servers into two separate columns, EzIP-unaware or EzIP-capable, to facilitate discussions that are to follow.

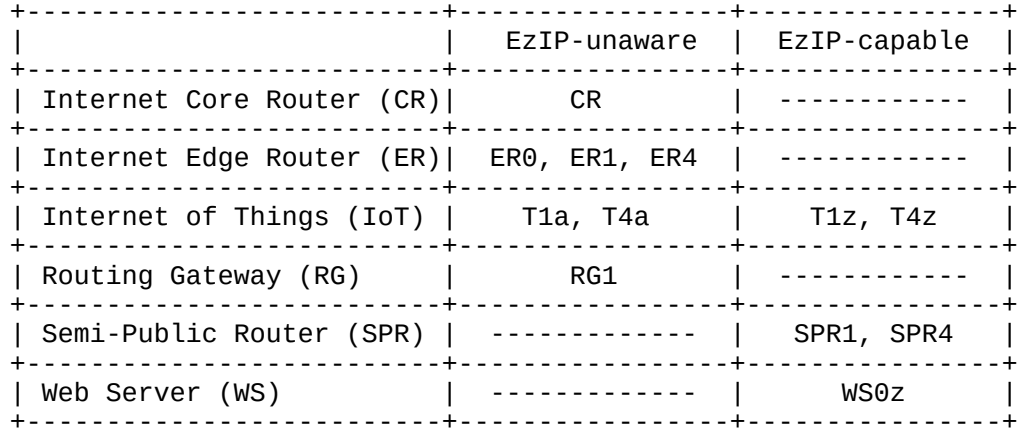

Figure 2 EzIP System Components

2.4. IP Header with Option Word

To transport the EzIP Extension Addresses through existing devices without being recognized as such and consequently acted upon, the IP Header Option mechanism defined by Figure 9 in Appendix A of [RFC791] is utilized to carry it as the payload. One specific aspect of its format deserves some attention. The meanings of the leading eight bits of each Option word, called "Opt. Code" or "Option-type octet", are summarized on Page 15 of [RFC791]. They are somewhat confusing because the multiple names used in the literature, and how

the octet is parsed into functional bit groups. For example, a two-digit hexadecimal number, "0x9A", is conventionally written in the binary bit string form as "1001 1010". As Opt. Code, however, the eight bits here are parsed into three groups of 1, 2 and 5 bits as "1 00 11010" with meanings described in Figure 3.

Meaning of EzIP ID = 0x9A (Example)		
Copy Bit	Class	Option Value / Number
1 (Set)	00 (Control)	11010 (26 - base 10)

Figure 3 Option Type Octet

A value of "1" for the first bit instructs all routers that this Option word is to be copied upon packet fragmentation. This reserves the Option word through such a process, if it is performed.

The value of "00" for the next two bits indicates that this Option word is for "Control" purpose.

The decimal "Option Value" of the last five bits, equaling to "26" is defined as the "Option Number" that is listed in the "Number" column of the Internet Protocol Version 4 (IPv4) Parameters list [11]. As can be seen there, "26" has not been assigned. Thus, it is temporarily used in this document to facilitate the EzIP presentation. The next unassigned Option Code, "0x9B" or Number "27" will also be tentatively utilized in this document.

2.5. Examples of Option Mechanism

The Option mechanism has been used for various cases. Since they were mostly for utility or experimental purposes, however, their formats may be remote from the incident topic. There were two cases specifically dealt with the address pool issues. They are referenced here to assist the appreciation of the Option mechanism.

A. EIP (Extended Internet Protocol) - Figure 1 of [RFC1385] [12] (Assigned but now deprecated Option Number = 17) by Z. Wang: This approach proposed to add a new network layer on top of the existing Internet for increasing the addressable space. Although equipment near the end-user would stay unchanged, those among the CRs apparently had to go through rather extensive upgrading procedures, perhaps due to the flexible length of the extended address (could be much longer than that of the IPv6).

B. EnIP (Enhanced IPv4) - Figure 1 of Internet Draft [13] (temporarily utilizing Option Number = 26) by W. Chimiak: This work made use of the three existing private network blocks to extend the public pool by trading the private network operation for end-to-end connectivity. The fully deployed EnIP will eliminate the current private networks which may be against the intuitive preference of end-users who have found the private network configuration quite desirable. For example, the RG-NAT serves as a rudimentary deterrent against intrusion. In addition, the coexistence of private RG-NAT and public EnIP router functions in the same EnIP devices (N1 & N2), could lead to certain logistic inconsistency concerns.

2.6. EzIP Header

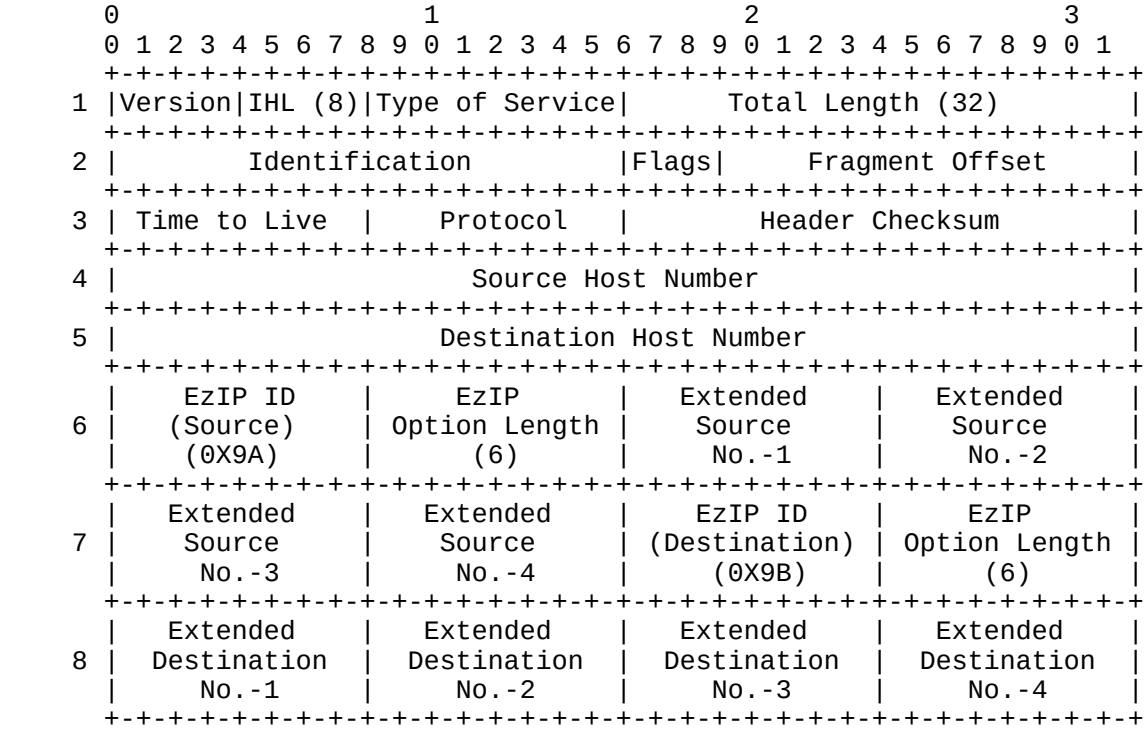

Figure 4 Full EzIP Header

The proposed EzIP header format shown in Figure 4 can transport the full 4 octet (32 bit) extension addresses of both ends of an Internet link. The extension addresses in the 240/4 netblock utilized in the EzIP scheme described herein have 28 significant bits. It is possible for EzIP to use addresses having other lengths

of significant bits for different multiplication factors. To prepare for such variations, two separate EzIP ID codes, "0x9A" and "0x9B" are proposed to distinguish between Source and Destination Option words, respectively, as basic examples.

2.7. EzIP Operation

To convey the general scheme, Appendix A presents examples of IP header transitions through routers, between IoTs with or without EzIP capability.

To introduce the EzIP approach into an environment where EzIP-unaware IoTs like T1a and T4a will be numerous for a long time to come, an SPR must be able to follow certain decision branches to determine how to provide the appropriate routing service for a smooth transition to the long-term operation. Appendix B outlines such logic and related considerations.

3. EzIP Deployment Strategy

Although the eventual goal of the SPR is to support both web server access by IoTs from behind private networks and direct end-to-end connectivity between IoTs, the former should be dealt with first to immediately mitigate the address shortage induced daily issues. In the process, the latter would be built up naturally.

A. Architecturally

Since the design philosophy of the SPR is an inline module between an ER and the private premises (RG or directly connected IoTs) that it serves, SPR introduction process can be flexible.

A.1. An SPR may be deployed as an inline module right after an ER to begin providing the CG-NAT equivalent function. This could be done immediately without affecting any of the existing Internet components, CR, ER and RG. EzIP-capable IoTs will then take advantage of the faster bi-directional routing service through the SPRs by initiating communication sessions utilizing EzIP headers to contact other EzIP-capable IoTs.

A.2. Alternatively, an SPR may be deployed as an adjunct module just before an existing RG or a directly connected IoT to realize the same EzIP functions on the private premises, even if the serving Internet Access Provider (IAP) has not enhanced its ERs with the EzIP capability.

This approach will empower individual communities to enjoy the new EzIP capability on their own by upgrading all Internet subscribers within a good-sized region to have publicly accessible EzIP addresses for intra-community peer-to-peer communication, starting from just using one existing public IPv4 address to identify the entire region through a gateway to the rest of the world. See sub-section C. below for more specific considerations.

B. Functionally

B.1. First, an IAP should install SPRs in front of business web servers so that new routing branches may be added to support the additional web servers for expanding business activities. Alternatively, this may be achieved if businesses on their own deploy new web servers with the SPR capability built-in.

B.2. On the subscriber side, SPRs should be deployed to disseminate static addresses to the public, and to facilitate the access to new web servers.

C. Regional Area Network

C.1. Since the size of the 240/4 netblock is significant, a region mentioned in sub-section A.2. above could actually be fairly large. Based on the assumption that each person, on the average, may have 6.6 IoTs by Year 2020 [3], a 240/4 netblock is capable of serving nearly 39M (256M / 6.6) individual devices, even before utilizing any private netblocks to manage private premises. This exceeds the population of the largest city on earth (38M - Tokyo Metro.) and 75% of the countries around the world (i.e., most of the 233 countries other than the top 35). Therefore, any finite sized region can immediately begin to enjoy EzIP addressing by deploying a Regional Area Network (RAN) utilizing SPRs operating with one 240/4 netblock of addresses from one IPv4 public address. With the gateway for a region configured in such a way that the entire region appears to be one ordinary IPv4 IoT to the rest of the Internet, a self-contained RAN may be deployed anywhere there is the need or desire, with no perturbation to the current Internet operations whatsoever.

C.2. This gateway may be constructed with a matured networking technology called Caching Proxy [14] popularized by data-intensive web services such as Google, Amazon, Yahoo, as well as gateways for corporate LANs, VPN (Virtual Private Network), etc. Developed for speeding up response to repetitive queries from a group of subscribers on the same topic, while storing data from the central data bank, caching proxies are placed at strategic locations close to potential high activities, essentially cloning the central data

bank into distributed copies (not necessarily a full set, but containing all relevant subsets pertaining to the local community). This architecture meshes with the EzIP-based RAN very well, because the address translation between the IPv4 in the Internet and the EzIP in the RAN can be accomplished transparently through the two ports of a caching proxy (For such matter, even could be between the IPv6 and the EzIP if desired!). Consequently, existing Internet routers, such as CR and ER may not see any IP packet with EzIP header at all, during the initial phase of the RAN deployment which will primarily consist of basic intra-regional messaging and web service access in a primarily local operation mode. Ongoing study of this possibility is reported in Appendix F.

C.3. This configuration actually mimics the PABX environment almost exactly. Since the entire region is only accessible through the gateway that performs the address translation, degenerated EzIP header (conventional IP header with words 4 and 5 using 240/4 netblock addresses) will be suffice for the intra RAN traffic. This mirrors the dialing procedure of using only extension numbers among stations served by the same PABX, circumventing the unnecessary and wasteful overhead of including the dialing of the common public telephone number prefix whose only purpose is to identify the PABX to the PSTN which is not involved in such intra-PABX communications.

C.4. The full EzIP header format will only be used when an EzIP-capable IoT intends to directly interact with an EzIP-capable IoT in another RAN. The last part is equivalent to the IDDD (International Direct Distance Dialing) conventions when a call is made through the PSTN to a station outside of a PABX.

C.5. The RAN would streamline the CIR (Country-based Internet Registry) model proposed by ITU-T [18] as well. Instead of allocating a block of public IPv6 addresses to an ITU-T authorized entity (essentially the sixth RIR - Regional Internet Registry) to administrate on behalf of individual countries, the EzIP RAN configuration enables each member state to start her own CIR with up to 256M IoTs, based on just one of the IPv4 public address already allocated to that country from the responsible RIR. Consequently, each CIR is coordinated by its parent RIR, yet its operation can conform to local preferences. This configuration will establish a second Internet service parallel to the existing one for demonstrating their respective merits independently, offering subscribers true options to choose from.

D. Permanently

In the long run, it would be best if SPRs are integrated into their host ER by upgrading the latter’s firmware to minimize the hardware and to streamline the equipment interconnections.

Appendix B details the considerations in implementing these outlines.

4. Updating Servers to Support EzIP

Although the IP header Option mechanism utilized by EzIP was defined a long time ago as part of the original IPv4 protocol [RFC791] [1], it has not been used much in daily traffic. Compatibility with current Internet facilities and conventions may need be reviewed. Since the EzIP data is transported as part of the IP header payload, it is not expected to affect higher layer protocols. However, certain facilities may have been optimized without considering the Option mechanism. They need be adjusted to provide the same performance to EzIP packets. There are also utility type of servers that need be updated to support the longer EzIP address. For example;

A. Fast Path

Internet Core Routers (CRs) are currently optimized to only provide the "fast-path" (through hardware line card) routing service to packets without Option word in the IP header [15]. This puts EzIP packets at a disadvantage, because EzIP packets will have to go through the "slow path" (processed by CPU’s software before giving to the correct hardware line card to forward), resulting in a slower throughput. Since the immediate goal of the EzIP is to ease the address pool exhaustion affecting web server access, subscribers not demanding high throughput performance may be migrated to the EzIP supported facility first. This gives CRs the time to update so that EzIP packets with authorized Option numbers will eventually be recognized for receiving the "fast-path" service. On the other hand, an alternative logic may be applied for the CR. That is, it should by default ignore any Option word in an IP header so that all IP packets will be processed through the "fast-path", unless a recognizable Option word requiring action is detected. This approach would mitigate the security issues caused by the "source routing" attack, as well.

B. Connectivity Verification

One frequently used probing utility for verifying baseline connectivity, commonly referred to as the "ping" function in PC terminology, needs be able to transport the full EzIP address that

is 64 bits long instead of the current 32-bit IPv4 address. There is an example of an upgraded TCP echo server in [RFC862] [16].

C. Domain Name Server (DNS)

Similarly, the DNS needs to expand its data format to transport the longer IP address created by the EzIP. This already can be done under IPv6. Utilizing the experimental IPv6 prefix 2001:0101 defined by [RFC2928] [17], EzIP addresses may be transported as standardized AAAA records.

These topics are discussed in more detail under an IETF Draft RFC, Enhanced IPv4 - V.03 [13].

5. EzIP Enhancement and Application

To avoid disturbing any assigned address, deployed equipment and current operation, etc., the EzIP scheme is derived under the constraint of utilizing only the reserved 240/4 address block. If such restriction were removed by allowing the entire IPv4 address pool be flexibly re-allocatable, the assignable public address pool could be expanded significantly more, as outlined below.

A. If the 240/4 netblock were doubled to 224/3, each existing IPv4 public address would be expanded by 512M fold. Since this block of 512M addresses have to be first reserved from the basic public pool, the resultant total addresses will be (4.096B - 512M) x 512M, or 1,835MB. This is over 36M times of the predicted number of IoTs (50B) by Year 2020. This calculation leads to additional possibilities.

B. The EzIP header in Figure 4, capable of transporting the full 32 bit IPv4 address, allows the extension number to be as long as practical. That is, we can go to the extreme of reserving only one bit for the network number, and using all the rest of bits for the extension address. With this criterion, the basic IPv4 pool may be divided into two halves, reserving one half of it (about 2B addresses) as a semi-public network with the network number prefix equal to "1". Each of the remaining 2B public addresses (with prefix equal to "0") of the basic IPv4 pool may then be extended 2B fold through the EzIP process, resulting in a 4BB address pool. This is roughly 80M times of the Year 2020 IoT needs.

C. If the EzIP technique were applied through several layers of SPRs in succession, the address expansion could be even more. For example, let’s divide the IPv4 pool equally into four blocks, each with about 1B addresses. Apply the first 1B address block to the

public routers. Set up three layers of SPRs, each makes use of one of the remaining three 1B address blocks. The resultant assignable pool will have 1BBBB addresses. Under this configuration, the full length of an IoT's identification code will be the concatenation of four segments of 32-bit IPv4 address, totaling 128 bits, the same as that of the IPv6. The first two bits of each segment, however, being used to distinguish from the other three address blocks, are not significant bits. This 8-bits difference makes the IPv6 pool 256 times larger. This ratio is immaterial, because even the 1BBBB address pool is already 20MBB times of the foreseeable need. It is the hierarchical addressing characteristics, made possible by the EzIP scheme, that will enhance the Internet, such as truncating out the common address prefix for communicating within a local community, and associating an address with the geographical position, thus mitigating the Geolocation related issues which have led to cyber security vulnerability.

D. Along this line of reasoning, we could combine two 1B address blocks together to be the basic public address. The overall assignable pool becomes 2BBB which is still 40MB times of the expected IoT need(50B). With this pool, we can divide the entire globe into 2B regions, each served by one public router. Each region can then be divided into 1B sections, identified by the first group of SPRs. Next, each section will have the second group of SPRs to manage up to 1B RGs and IoTs. Since the basic 2B public addresses are already more than half of the current total assignable IPv4 public addresses (3.84B), their potential Geolocation resolution capabilities are comparable. With additional two layers of SPR routing, 1B for each, the address grid granularity will be so refined that locating the source of an IP packet becomes a finite task, leaving perpetrators little room to hide.

E. The following outlines a possible procedure for optimizing the use of the EzIP address resource by transforming the current Internet to be a Geolocation-capable address system while maintaining the existing IPv4 addressing and operation conventions:

a. Quantitative Reference: IETF [RFC6598] [6] reserved the 100.64/10 block with 4M addresses for supporting IAP's CG-NAT service. Applying all of these to the entire IPv4 pool of 4B addresses, the maximum effective CG-NAT supported IPv4 address pool could be 16MB. This is 0.32M times of the expected number (50B) of IoTs by Year 2020.

b. Employing the 240/4 netblock with 256M addresses in the EzIP extension scheme, a /6 block with 64M addresses from the IPv4

basic public pool is sufficient to replicate the above 16MB capacity. This frees up the majority of the IPv4 public pool.

c. Since this will be a temporary holding pool to release the current addresses for new assignments, it should occupy as few public addresses as possible to leave the maximum number of addresses for facilitating the long-term planning. To just support the expected 50B IoTs need, only 200 IPv4 public addresses are required (200 x 256M = 50B). Thus, a /24 block with 256 addresses is more than enough to accommodate this entire migration process. This frees up even more IPv4 public addresses.

d. Although a single /24 public address block is sufficient for migrating all currently perceived IPv4 address needs into one compact temporary EzIP pool, world-wide coordination of new address assignments and routing table updates will be required. It will be more expeditious to carry out this preparatory phase on an individual country or geographical region basis utilizing public IPv4 addresses already assigned to that area and actively served by existing CR routing tables. Since 200 public addresses are enough to port the entire IoT addresses, most of the 233 countries other than the top 35 (about 75%) countries should be able to port all of their respective predicted IoTs to be under one 240/4 netblock, each represented by one gateway to the Internet. If this is managed according to geographical disciplines, each participating region will begin to enjoy the benefits of the EzIP approach, such as plentiful assignable public addresses, robust security due to inherent Geolocation ability to spot hackers from within, so that efforts may be focused on only screening suspicious packets originated from without.

e. As IoTs are getting migrated to the temporary pool, the IPv4 addresses they originally occupy shall be released to re-populate the public address pool for establishing full scale EzIP operation.

f. Upon the completion of the EzIP based world-wide public address allocation map, each country can simply give up the few temporary public addresses in exchange for the permanent assignments. Since the latter is likely more than the former, addresses in one 240/4 netblock will be served by two (or more) 240/4 netblocks. Then, each of such 240/4 netblock will have more than half of its capacity available to serve the growth of additional IoTs.

g. This last step is very much the same as the traditional PSTN "Area Code Split" practice, whereby telephone numbers of a

service area are split into two (or more) blocks, upon introducing one (or more) new area code(s) into the area. All subscribers will continue to use their original local telephone numbers for calling among neighbors daily, except some may be assigned with a new area code prefix. Upon the split, each area code will have more than half of its assignable telephone numbers available to support the future subscriber growth within its service area. Mimicking the PSTN, the EzIP based Internet will have similar Geolocation capability as the former's caller identification-based services, such as the 911 emergency caller location system in US, mitigating the root cause to the cybersecurity vulnerability.

F. With the IPv4 address shortage issue resolved, potential system configurations utilizing the EzIP enhanced address pool may be explored.

a. Although the entire predicted number (50B) of IoTs by Year 2020 may be served by just one /24 IPv4 public address block utilizing the EzIP scheme with a 240/4 netblock, let's replace it with a /8 block (16M addresses), resulting in about 4MB (16M x 256M) assignable addresses. This is 80K times of the expected 50B IoTs. Or, each and every person (of predicted 2020 population) would have to own over 500K IoTs to use up this address pool. It is apparent that the spares in this allocation should be sufficient to support the growth of the IoTs for some years to come.

b. Next, the IPv4 pool originally has 256 blocks of /8 addresses. After the above allocation, there are still 239 blocks of /8 addresses available to support additional digital communication systems, each having the same size of address pool as the allocation above. Consequently, many world-wide communication networks may coexist under the same IPv4 protocol framework in the form of groups of RANs as described earlier, with arm's-length links among them.

c. For example, a satellite-based Internet that is being proposed [19], such as StarLink can start fresh as one EzIP RAN served by one SPR having the capacity of 256M IoTs, under one ER capable of managing one /8 block of IPv4 public address. Utilizing a caching proxy as the gateway to handle the data exchange with other RAN, this satellite-based Internet with 256M hosts can operate pretty much as an isolated system by using 240/4 addresses in the basic IP headers for intra-RAN communications, most of the time. Only when direct communication with another RAN (such as the one for the existing Internet) is needed, will the full EzIP header be required. As users grow, additional RANs (each with 256M IoTs capacity), may be incrementally added to support the expansion.

G. In summary, utilizing the 240/4 netblock, the EzIP scheme may expand the IPv4 based Internet to be a collection of up to 240 groups of 16M RANs each managed by one SPR with 256M IoTs capacity that are inter-operable digital communication systems, normally operate at arm’s-length to one another. Each of these groups has the address capacity of at least 80K times of the number of predicted (50B) IoTs by Year 2020.

6. Security Considerations

EzIP solution is based on an inline module called SPR that is intended to be as transparent to Internet traffic as possible. The proposed address assignment rule is deterministic and systematic. Thus, no overall system security degradation is expected.

7. IANA Considerations

Being an overlay to the existing Internet fabric, each RAN behaves as an isolated island where a 240/4 netblock is used. Such a private use will not clash with any existing unicast addresses and is independent of any activity beyond each respective RAN including the reuse of the 240/4 block in another RAN. Therefore, the existing classification of "Reserved for Future Use" for 240/4 would be just fine. It doesn’t require any particular IANA re-designation of the address block.

However, to avoid the continued confusions due to the indeterministic nature of the current classification, this draft requests IANA to re-designate the 240/4 netblock as unicast and in particular to be grouped under RFC6598 as its second netblock resources for enhancing CG-NAT type of services.

8. Conclusions

To resolve the IPv4 public address pool exhaustion issue, a technique called EzIP (phonetic for Easy IPv4) making use of a long-reserved address block 240/4, is proposed.

This draft RFC describes an enhancement to IPv4 operation utilizing the IP header Option mechanism defined in [RFC791]. Since the design criterion is to enhance IPv4 by extending instead of altering it, the impact on already in-place routers and security mechanisms is minimized.

The basic EzIP philosophy includes maintaining the existing public and private network structure. Upon reclassifying the "RESERVED for Future use" 240/4 netblock to be the Semi-Public address pool, it

will only be usable by the new SPR (Semi-Public Router) as the EzIP extension address. This pool can multiply each current IPv4 public address by 256M fold, while all existing public network and subscriber premises setups (private networks as well as directly connected IoTs) may remain unchanged. A subscriber is encouraged to upgrade his IoT(s) to be EzIP-capable so as to fully enjoy the enhanced router service by EzIP for end-to-end communication. This particular manifestation of the EzIP scheme appears to be the optimal solution to our needs.

The 240/4 netblock based EzIP scheme will not only relieve the IPv4 address shortage, but also improve the defense against cybersecurity intrusion by virtue of systematic and deterministic address management. The EzIP RAN configuration will also support the desire to establish CIR (Country-based Internet Registry) operation expressed by ITU-T, as a parallel local facility providing services equivalent to those of the current global Internet.

Furthermore, EzIP will help the IPv4 based Internet to become the common backbone for multiple world-wide digital communication systems such as satellite-based systems like StarLink that normally would operate in arm’s-length from one another.

These last two possible applications turn out to be a generic architectural feature that is also suitable for establishing test beds at arm’s-length to one another for developing new protocols and products. This particular manifestation of the EzIP empowers end-users to participate in the evaluation, and the smooth transition from testing to the eventual use, of new services in a realistic, not simulated, parallel environment.

9. References

9.1. Normative References

[1] https://datatracker.ietf.org/doc/html/rfc791

[2] https://datatracker.ietf.org/doc/html/draft-wilson-class-e-02

9.2. Informative References

[3] https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf

[4] https://stats.labs.apnic.net/ipv6

[5] https://stats.ams-ix.net/sflow/ether_type.html

[6] https://datatracker.ietf.org/doc/html/rfc6598

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

[8] https://datatracker.ietf.org/doc/html/rfc1918

[9] https://datatracker.ietf.org/doc/html/rfc793

[10] https://www.ietf.org/rfc/rfc2131.txt

[11] https://www.iana.org/assignments/ip-parameters/ip-parameters.xhtml

[12] https://datatracker.ietf.org/doc/html/rfc1385

[13] https://datatracker.ietf.org/doc/html/draft-chimiak-enhanced-ipv4-03

[14] https://en.wikipedia.org/wiki/Proxy_server#Improving_performance

[15] https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.477.1942&rep=rep1&type=pdf

[16] https://datatracker.ietf.org/doc/html/rfc862

[17] https://datatracker.ietf.org/doc/html/rfc2928

[18] https://www.nro.net/wp-content/uploads/nro-response-to-ls-5.pdf

[19] https://www.commerce.senate.gov/2017/10/the-commercial-satellite-industry-what-s-up-and-what-s-on-the-horizon

10. Acknowledgments

The authors would express their deep appreciation to Dr. W. Chimiak for the enlightening discussions about his team’s efforts and experiences through their EnIP development.

This document was prepared using 2-Word-v2.0.template.dot.

Appendix A. EzIP Operation

To demonstrate how EzIP could support and enhance the Internet operations, the following are three sets of examples that involve SPRs as shown in Figure 1. These present a general perspective of how IP header transitions through the routers may look like.

1. The first example is between EzIP-unaware IoTs, T1a and T4a. This operation is very much the same as the conventional TCP/IP packet transmission except with SPRs acting as an extra pair of routers providing the CG-NAT service.

2. The second one is between EzIP-capable IoTs, T1z and T4z. Here, the SPRs process the extended semi-public IP addresses in router mode, avoiding the drawbacks due to the CG-NAT type of table look-up operations above.

3. The last one is between EzIP-unaware and EzIP-capable IoTs. By initiating and responding with a conventional IP header, EzIP-capable IoTs behave like EzIP-unaware IoTs. Thus, all packet exchanges use the conventional IP headers, just like case 1. above.

A.1. Connection between EzIP-unaware IoTs

A.1.1. T1a Initiates a Session Request towards T4a

T1a sends a session request to SPR4 that serves T4a by a plain IP packet with header as in Figure 5, to RG1. There is no TCP port number in this IP header yet.

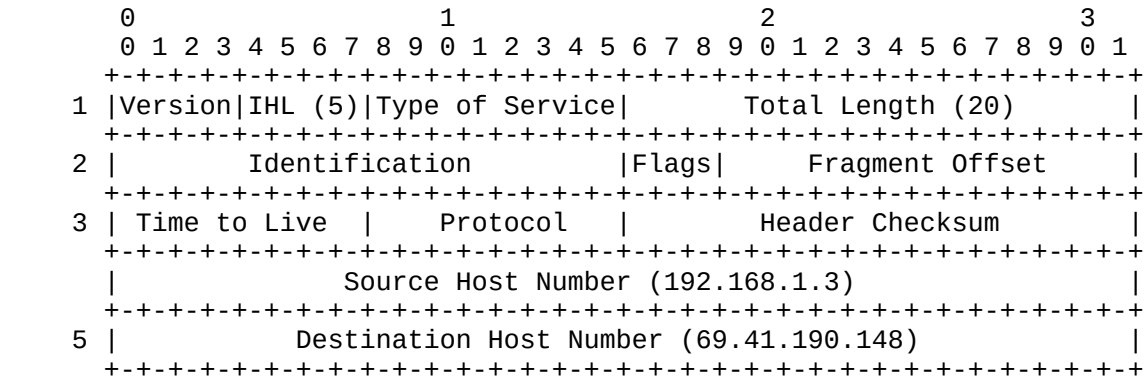

Figure 5 IP Header: From T1a to RG1

A.1.2. RG1 Forwards the Packet to SPR1

RG1, allowing be masqueraded by T1a, relays the packet toward SPR1 by assigning the TCP Source port number, 3N, to T1a, with a header as in Figure 6. Note that the suffix "N" denotes the actual TCP port number assigned by the RG1's RG-NAT. This could assume multiple values; each represents a separate communications session that T1a is engaged in. A corresponding entry is created in the RG1 state table for handling the reply packet from the Destination site. Since T4a's TCP port number is not known yet, it is filled with all 1's.

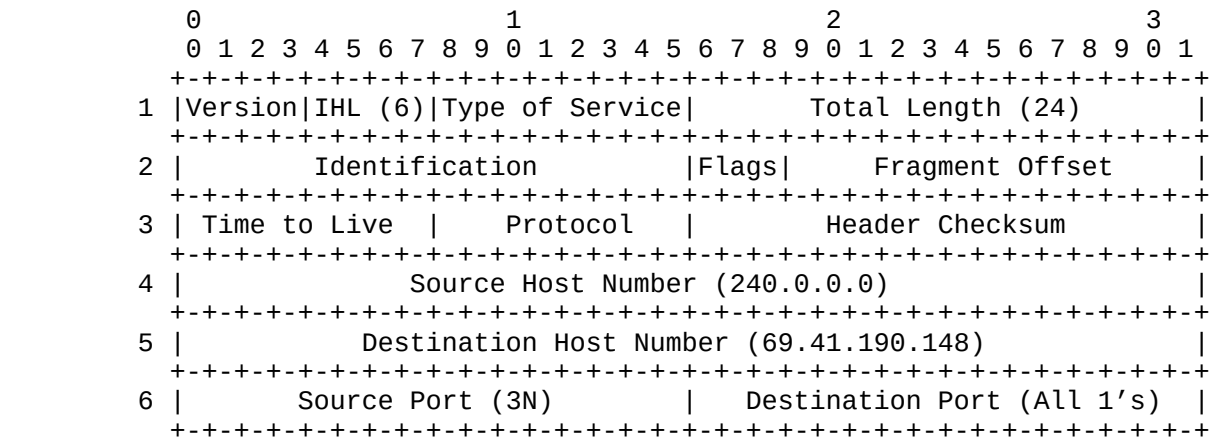

Figure 6 TCP/IP Header: From RG1 to SPR1

A.1.3. SPR1 Sends the Packet to SPR4 through the Internet

SPR1, detecting no EzIP Option word, acts like a CG-NAT. It allows being masqueraded by RG1 (with the Source Host Number changed to be SPR1's own and the TCP port number changed to 0C, where "0" is the last octet of RG1's IP address, and "C" stands for CG-NAT) and sends the packet as in Figure 7 out through the Internet towards SPR4. The packet traverses through the Internet (ER1, CR and ER4) utilizing only the Destination Host Number (word 5) in the header.

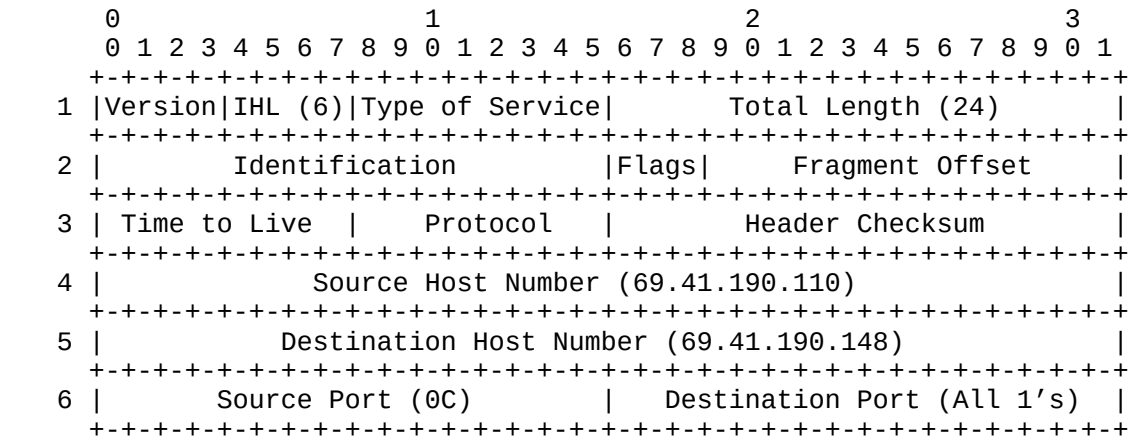

Figure 7 TCP/IP Header: From SPR1 to SPR4

Note that although schematically shown in Figure 1 as one public IPv4 address serving one SPR capable of a full 240/4 address block, the PCP port number has a theoretical limit of 64K (256 x 256) because it consists of 16 bits. This is much smaller than a full 240/4 pool. Even with dynamic assignments, it will take quite a few public addresses to serve the CG-NAT need if many IoTs are EzIP-unaware. So, IoTs are encouraged to become EzIP-capable as soon as possible to avoid straining the SPR's CG-NAT capability. This should not be an issue for emerging regions currently having very little facility and IoTs. As new ones are deployed, they should be enabled as EzIP-capable by factory default. For the rural area of developed countries with existing EzIP-unaware IoTs, the need for CG-NAT service will be greater. Multiple IPv4 public addresses would be needed initially to support smaller sub- 240/4 netblocks. This is probably workable because the latter does have more public IPv4 addresses. The CG-NAT techniques developed under [RFC6598] [6] may be incorporated here to facilitate the transition.

A.1.4. SPR4 Sends the Packet to T4a

Since the packet has a conventional TCP/IP header without Destination TCP port number, SPR4 would ordinarily drop it due to the CG-NAT function. However, for this example, let’s assume that there exists a state-table that was set up by a DMZ (De-Militarized Zone) process for redirecting this packet to T4a with a CG-NAT TCP port number 10C (Here, "10" is the fourth octet of T4a’s Extension address, and "C" stands for CG-NAT.). After constructing the Destination Host Number accordingly, SPR4 sends the packet to T4a with a header as in Figure 8.

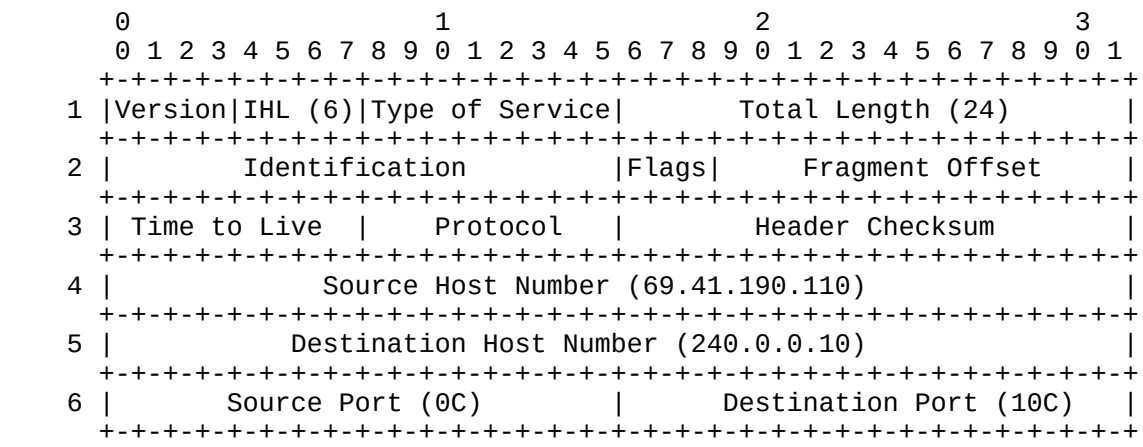

Figure 8 TCP/IP Header: From SPR4 to T4a

A.1.5. T4a Replies to SPR4

T4a interchanges the Source and Destination identifications in the incoming TCP/IP packet to create a header as in Figure 9, for the reply packet to SPR4.

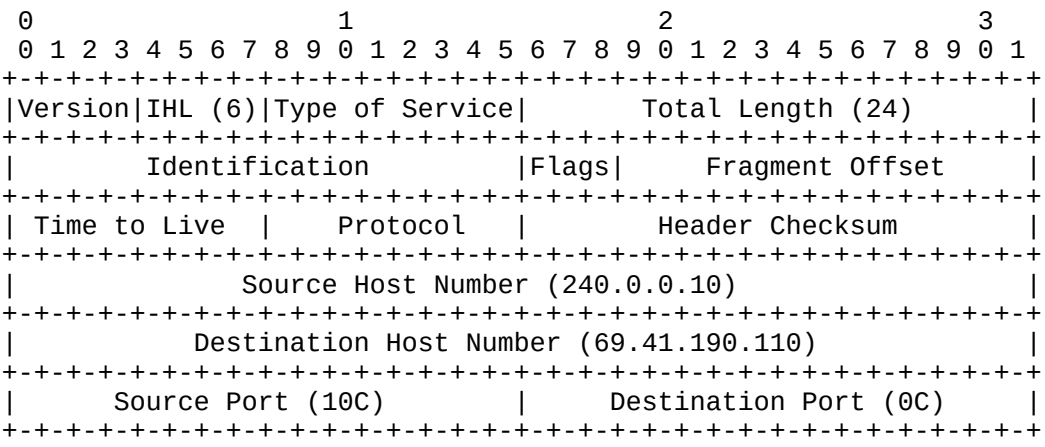

Figure 9 TCP/IP Header: From T4a to SPR4

A.1.6. SPR4 Sends the Packet to SPR1 through the Internet

SPR4, allowing being masqueraded by T4a, sends the packet toward SPR1 with the header in Figure 10, through the Internet (ER4, CR and ER1) who will simply relay the packet according to the information in word 5 (Destination Host Number):

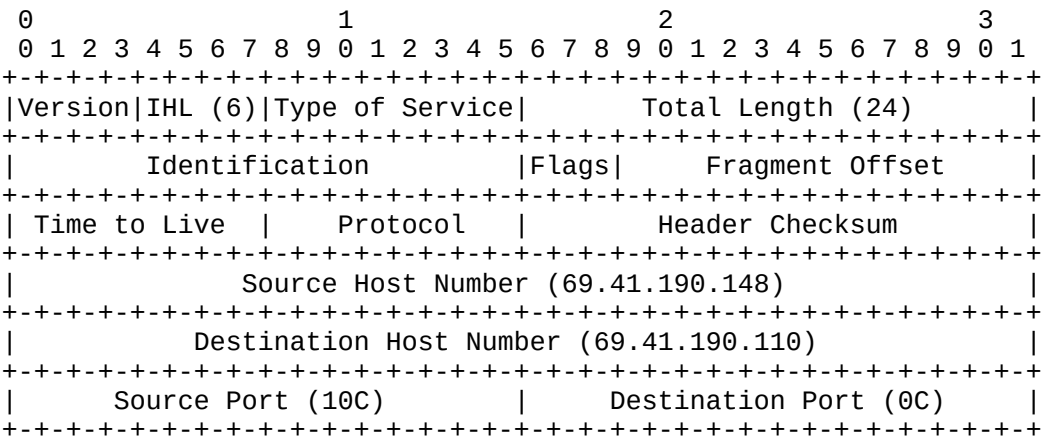

Figure 10 TCP/IP Header: From SPR4 to SPR1

A.1.7. SPR1 Sends the Packet to RG1

Using the stored data in the CG-NAT state-table, SPR1 reconstructs a header as in Figure 11, for sending the packet to RG1.

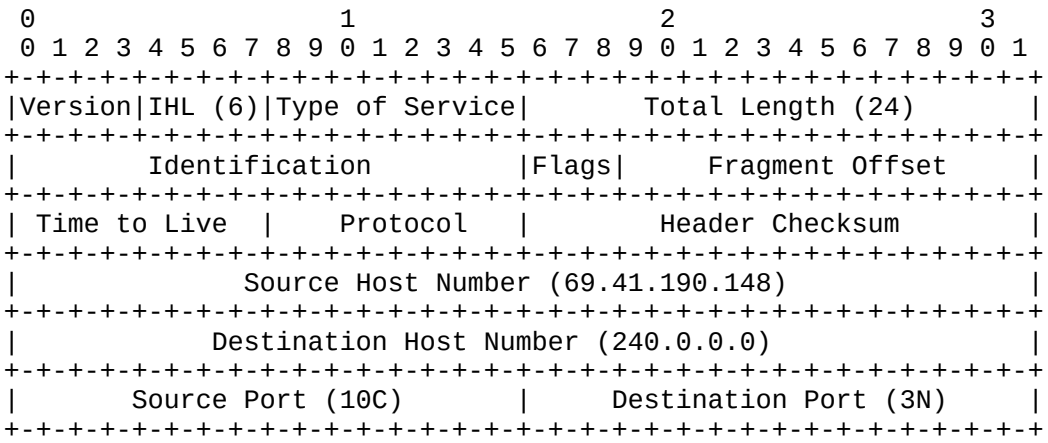

Figure 11 TCP/IP Header: From SPR1 to RG1

A.1.8. RG1 Forwards the Packet to T1a

From the state-table in RG1's RG-NAT, T1a address is reconstructed based on Destination Port (3N), as in Figure 12.

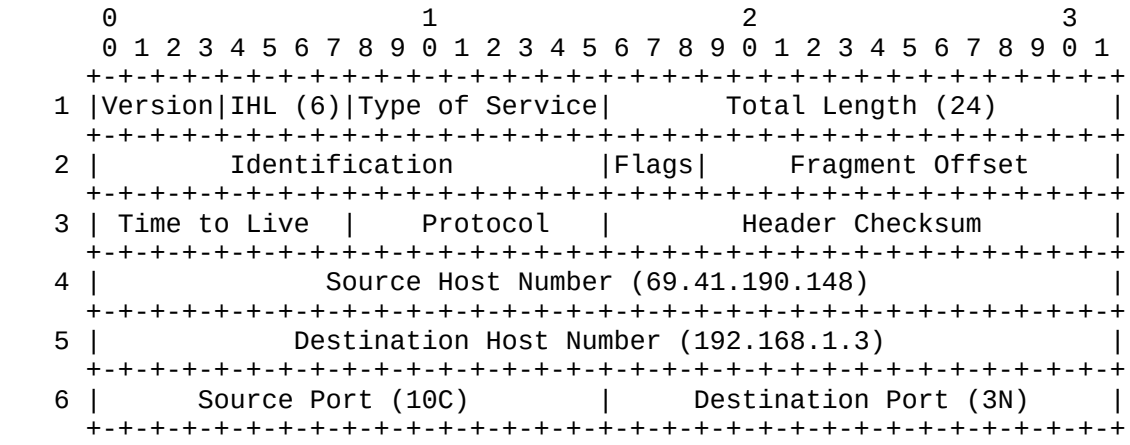

Figure 12 TCP/IP Header: From RG1 to T1a

A.1.9. T1a Sends a Follow-up Packet to RG1

To carry on the communication, T1a constructs a full TCP/IP header as Figure 13 for sending the follow-up packet to RG1.

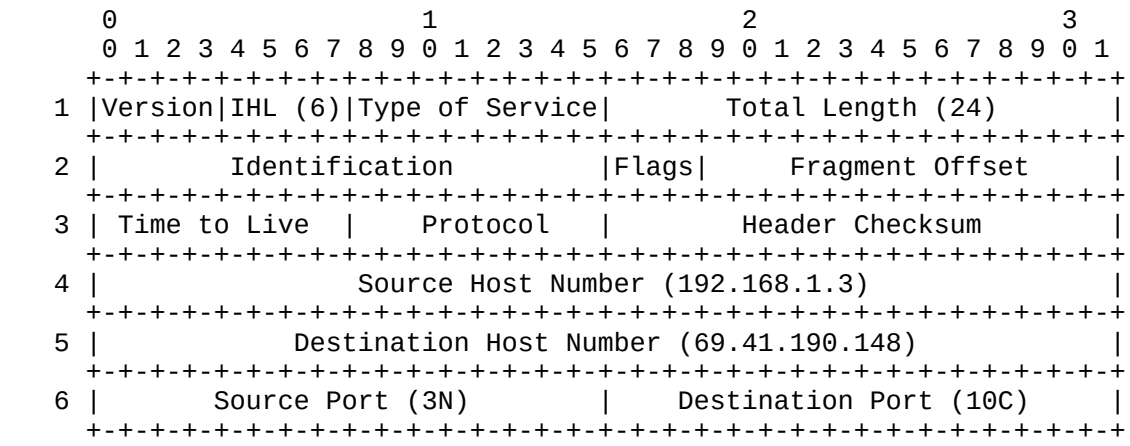

Figure 13 TCP/IP Header: Follow-up Packets From T1a to RG1

A.2. Connection Between EzIP-capable IoTs

The following is an example of EzIP operation between T1z and T4z shown in Figure 1, with full "Public - EzIP : Private" network addresses, "69.41.190.110-240.0.0.0:9" and "69.41.190.148-246.1.6.40", respectively. Note that T4z, without the private portion (TCP port number) in the concatenated address, is directly addressable from the Internet. For T1z to initiate a session, it needs to know the full address of T4z, but only its own private address.

A.2.1. T1z Initiates a Session Request towards T4z

T1z sends an EzIP packet, as in Figure 14, to RG1. There is no TCP port number word, because T4z does not have such while that for T1z is waiting for assignment from the RG1's RG-NAT. Also, the Extended Source No. is filled with all "1's", waiting for being specified by SPR1.

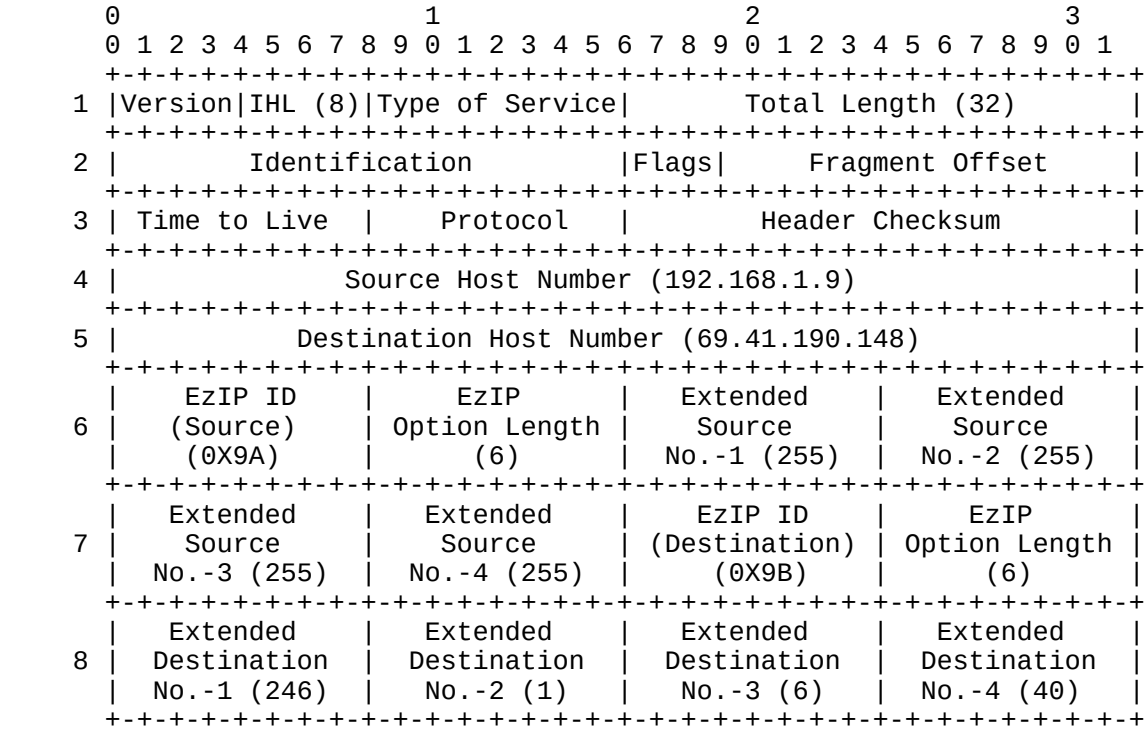

Figure 14 EzIP Header: From T1z to RG1

A.2.2. RG1 Forwards the Packet to SPR1

RG1, allowing to be masqueraded by T1z, relays a packet as in Figure 15, toward SPR1 by assigning the TCP Source port number, 9N, to T1z. Not knowing whether T4z is behind an RG, "All 1's" is used to fill the Destination Port part of the TCP word.

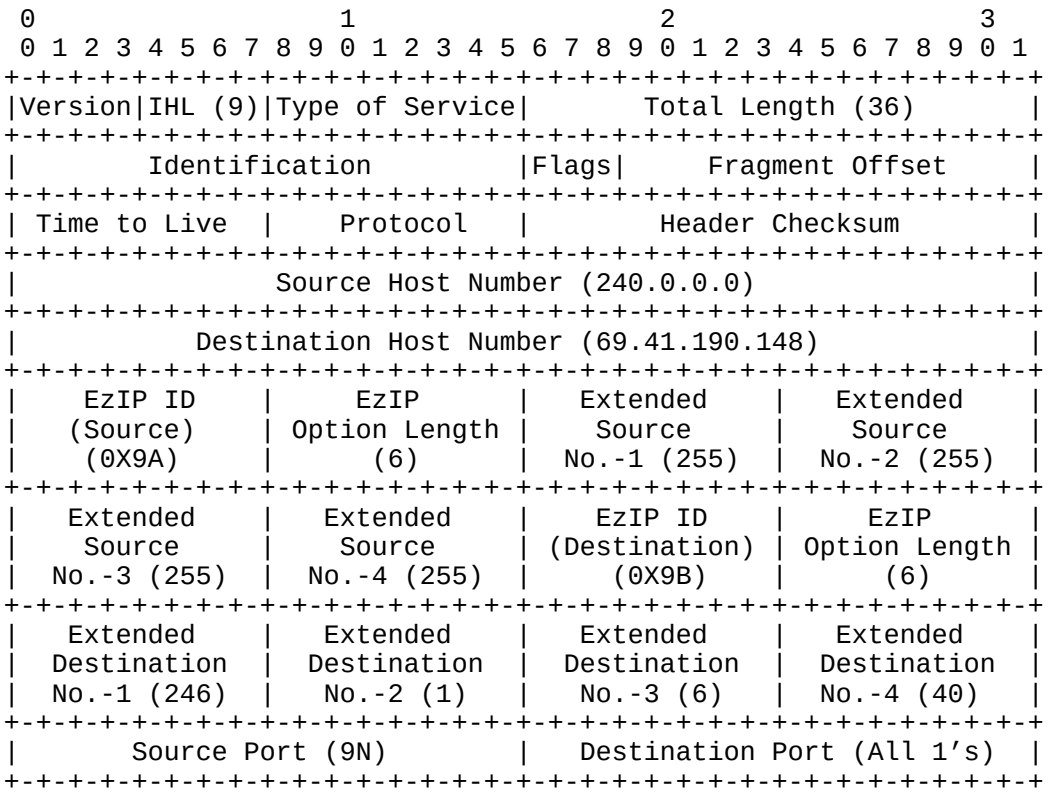

Figure 15 TCP/EzIP Header: From RG1 to SPR1

A.2.3. SPR1 Sends the Packet to SPR4 through the Internet

SPR1 replaces the Source Host Number with its own as well as fills in the Extended Source No. information, and then sends the packet, with a header as in Figure 16, out into the Internet towards SPR4. The packet traverses through ER1, CR and ER4, utilizing only the Destination Host Number (Word 5) in the IP Header.

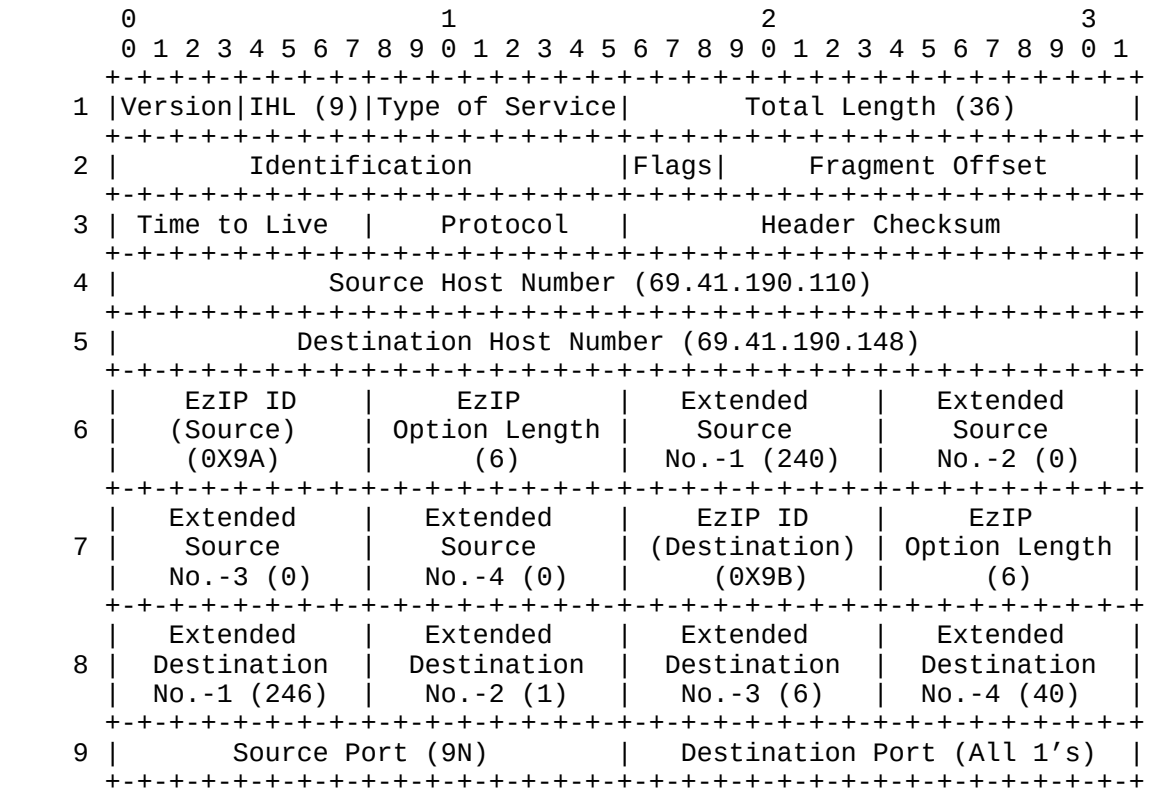

Figure 16 TCP/EzIP Header: From SPR1 to SPR4

A.2.4. SPR4 Sends the Packet to T4z

SPR4 reconstructs T4z address from the Option number 0X9B and the Extended Destination No. then sends the packet, with the header as in Figure 17, to T4z.

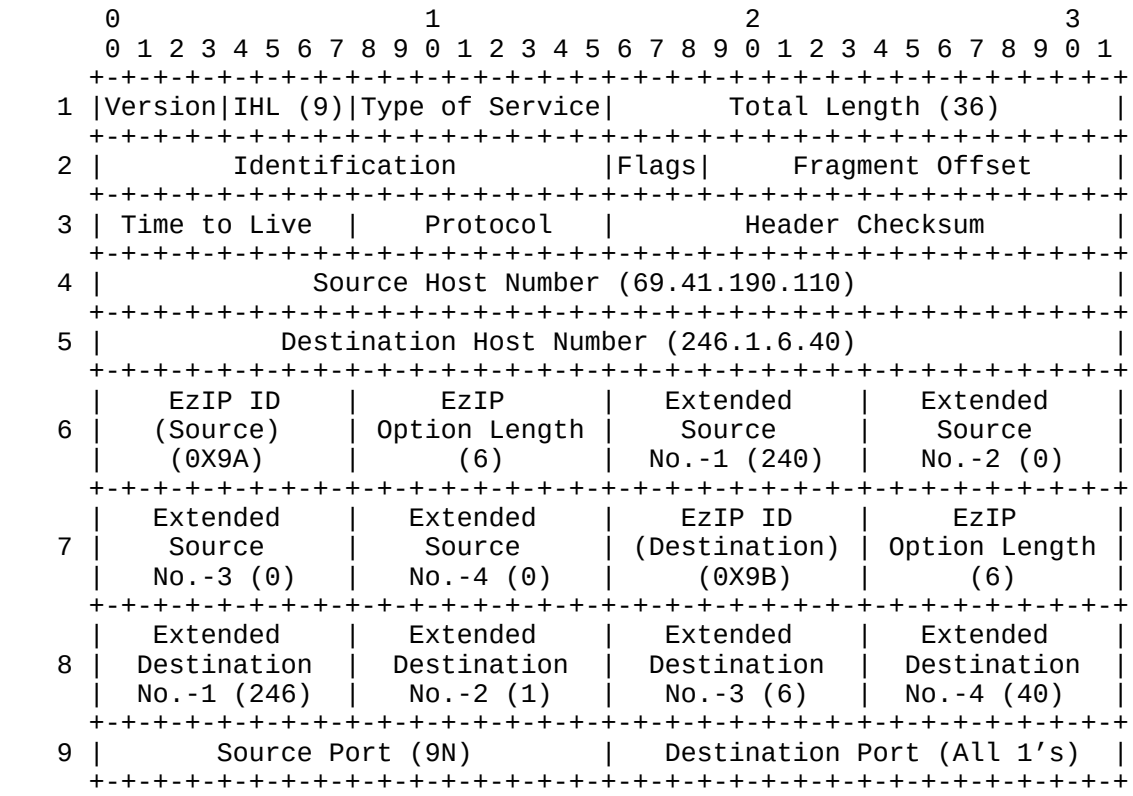

Figure 17 TCP/EzIP Header: From SPR4 to T4z

A.2.5. T4z Replies to SPR4

Making use of the information in the incoming TCP/EzIP header, T4z replies to SPR4 with a full header, as in Figure 18.

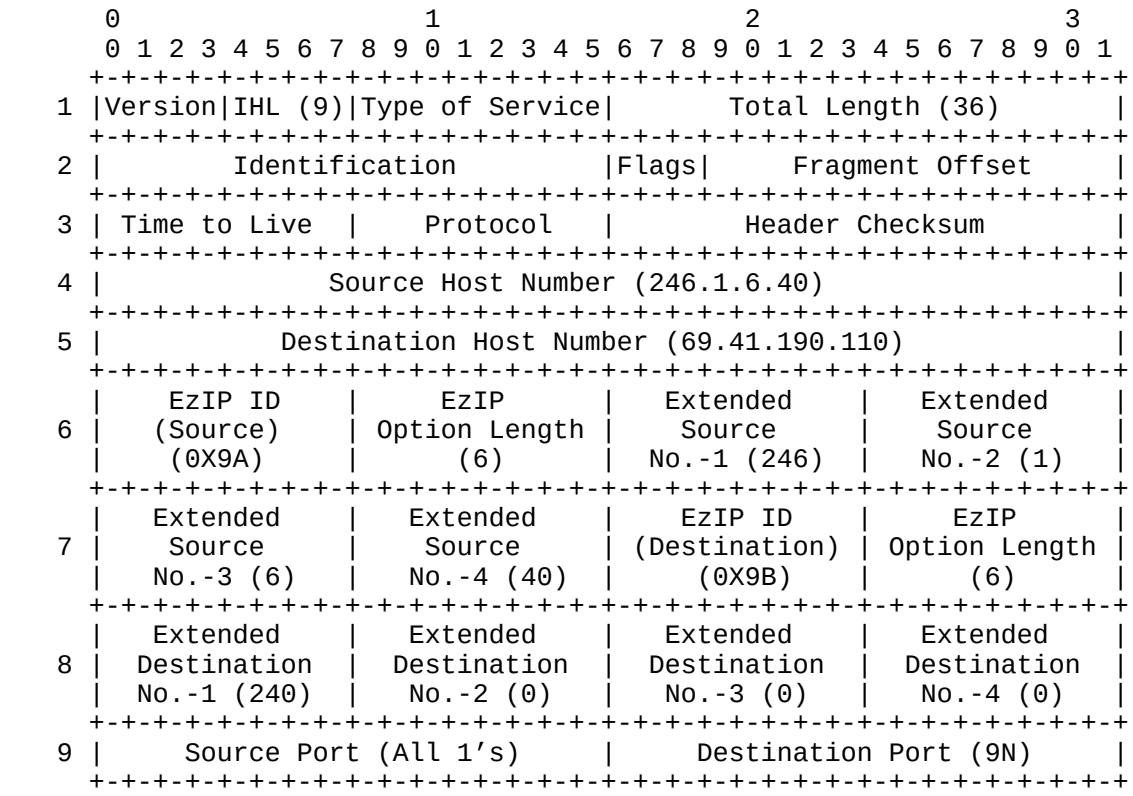

Figure 18 TCP/EzIP Header: From T4z to SPR4

A.2.6. SPR4 Sends the Packet to SPR1 through the Internet

SPR4 replaces the Source Host Number with its own, and sends the packet with the header, as in Figure 19, towards SPR1. The Internet (ER4, CR, and ER1) simply relays the packet according to the TCP/EzIP header word 5 (Destination Host Number):

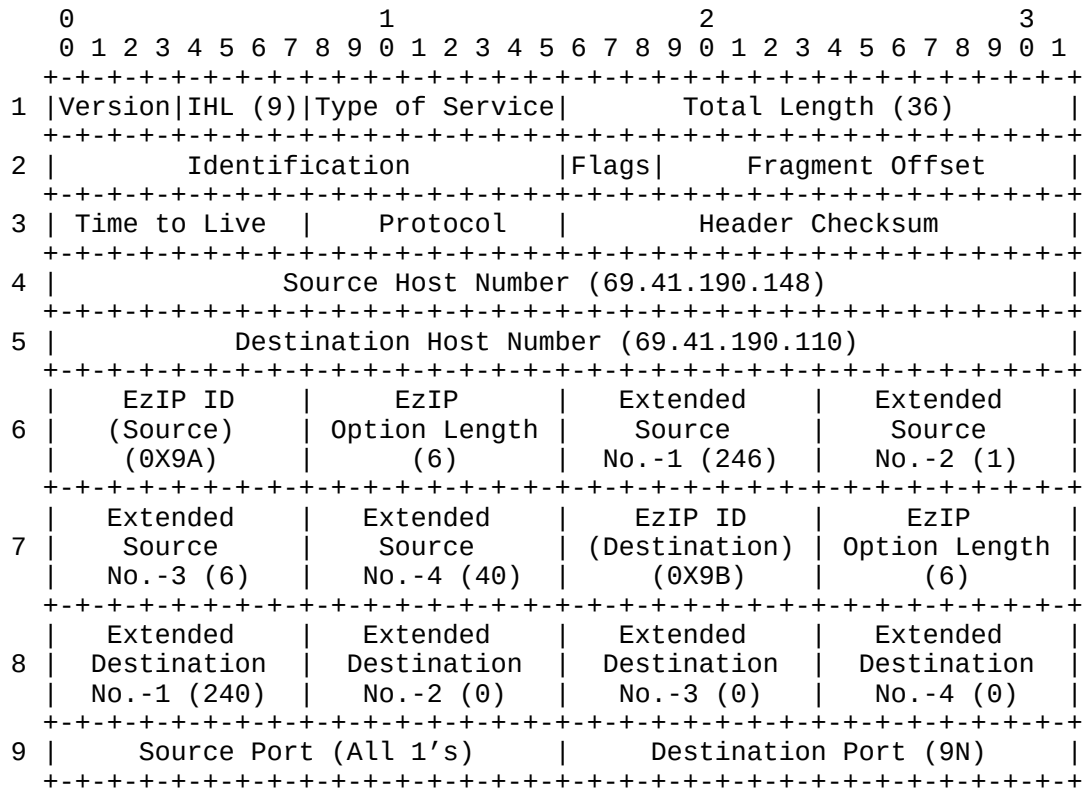

Figure 19 TCP/EzIP Header: From SPR4 to SPR1

A.2.7. SPR1 Sends the Packet to RG1

SPR1 reconstructs RG1 address from the Option number 0X9B and the Extended Destination No. Then, sends packet with a header as in Figure 20 toward RG1.

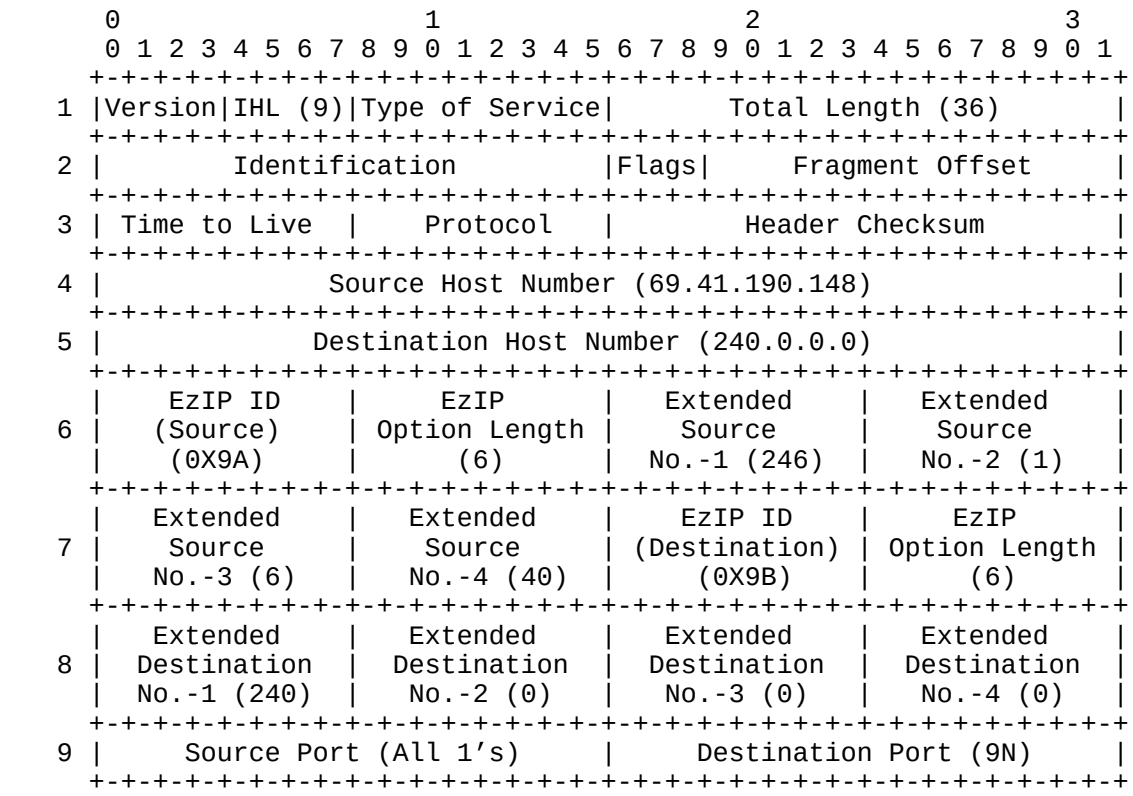

Figure 20 TCP/EzIP Header: From SPR1 to RG1

A.2.8. RG1 Forwards the Packet to T1z

RG1 reconstructs T1z address from RG1's RG-NAT state-table based on Destination Port (9N), then sends the packet to T1z with a header as in Figure 21.

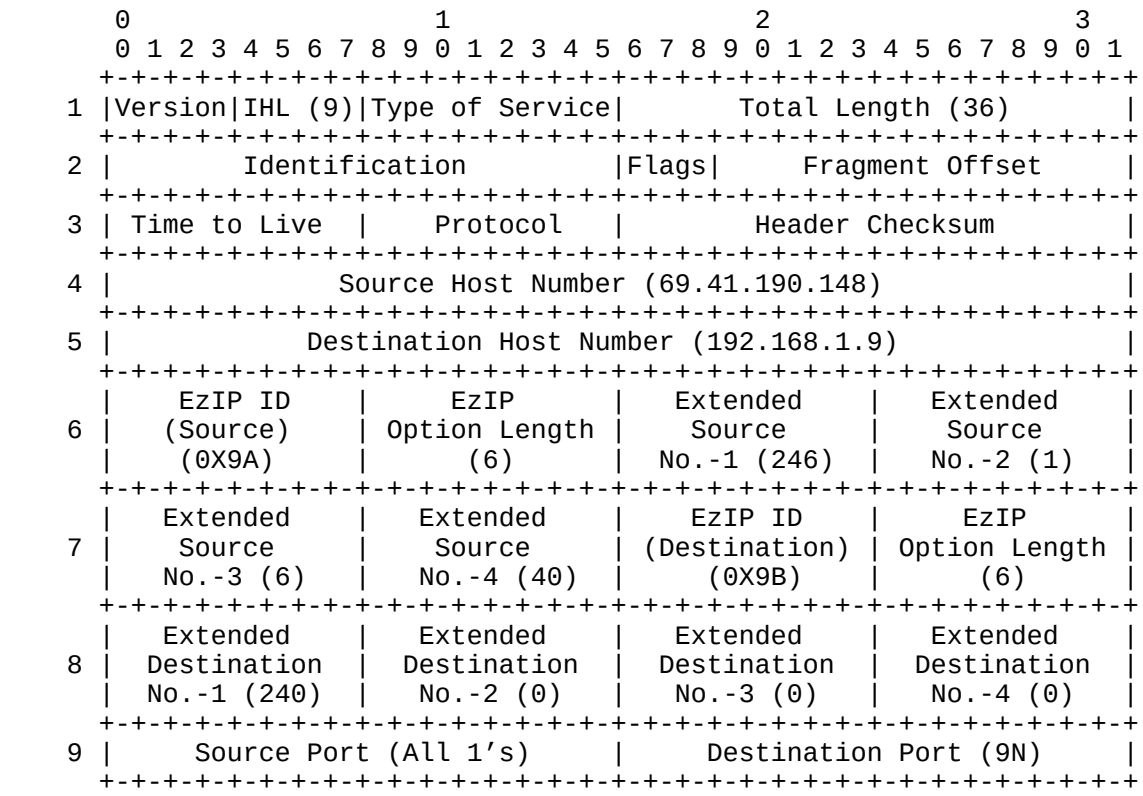

Figure 21 TCP/EzIP Header: From RG1 to T1z

A.2.9. T1z Sends a Follow-up Packet to RG1

With all fields filled with needed information from the incoming TCP/EzIP header, T1z sends a follow-up packet to RG1 as in Figure 22.

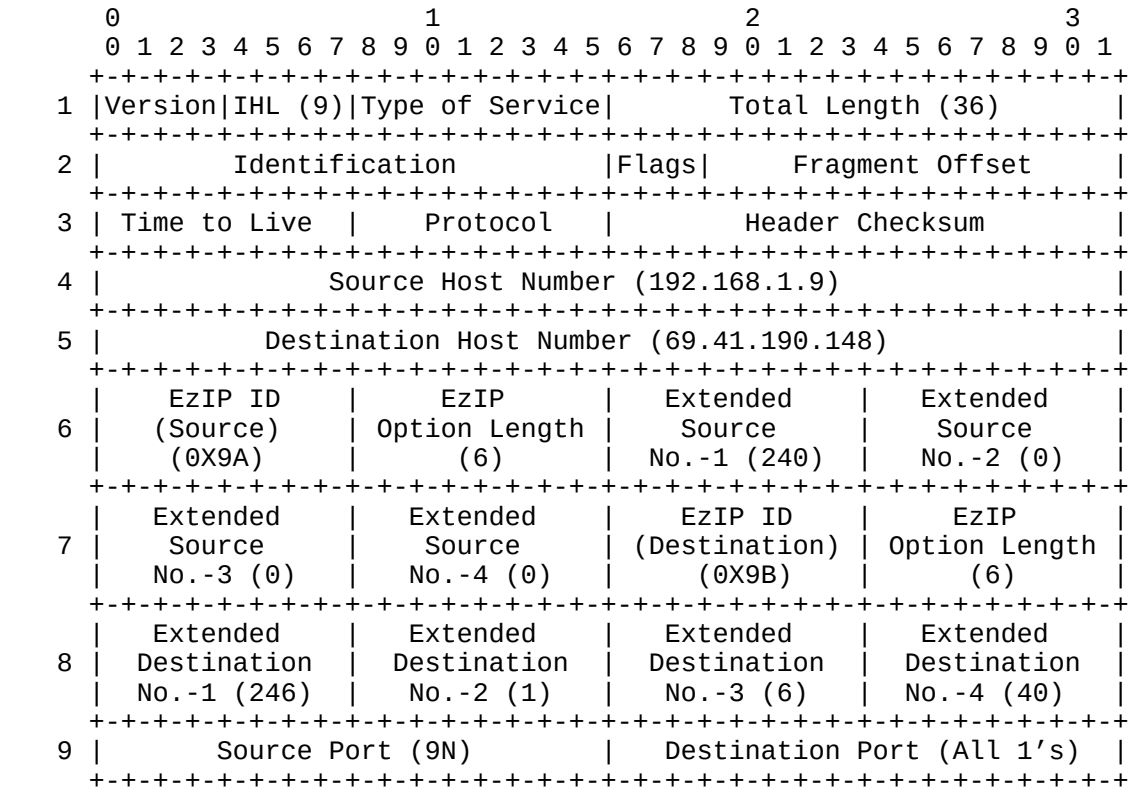

Figure 22 TCP/EzIP Header: Follow-up Packets from T1z to RG1

A.3. Connection Between EzIP-unaware and EzIP-capable IoTs

A.3.1. T1a Initiates a Request to T4z

Since T1a can create only conventional format IP header, the SPRs will provide CG-NAT type of services to the TCP/IP packets. And, assuming SPR4 has a state-table set up by DMZ for forwarding the request to T4z, the packet will be delivered to T4z. Seeing the incoming packet with conventional TCP/IP header, T4z should respond with the same so that the session will be conducted with conventional TCP/IP headers. The interaction will follow the same behavior as in Appendix A.1.

A.3.2. T1z Initiates a Request to T4a

Knowing T4a is not capable of EzIP header, T1z purposely initiates the request packet using conventional IP header. It will be treated by SPRs in the same manner as the T1a initiated case as in Appendix A.1., so that the packet will be recognizable by T4a.

Note that to maximize the combination in the EzIP System Architecture diagram (Figure 1) for demonstrating the possible variations, there is no RG on Premises 4. IoTs, such as T4a and T4z, are thus directly connected to a SPR, like SPR4 and there is no corresponding TCP port number in word 9 of the above TCP/EzIP headers. This spare facility in the header suggests that an RG may be installed if desired, to establish the similar private network environment as that on Premises 1.

In brief, the steps outlined above are very much the same as the conventional TCP/IP header transitions through the Internet with the SPR providing the CG-NAT service. Except, when a TCP/EzIP header is detected, the SPR switches to the router mode for forwarding the packet to improve the performance.

In essence, with the EzIP system architecture very much the same as today’s Internet, the SPR starts with assuming the current CG-NAT duty, while ready to perform the new EzIP routing function for EzIP-aware IoTs. This strategy offers a simple transition path for the Internet to evolve toward the future.

It is important to note that both SPR and CG-NAT are inline devices with respect to ER. However, since CG-NAT provides soft / ephemeral TCP ports, it is positioned between a CR and ERs, while SPR is located between an ER and RGs to assign hard / static physical addresses.

Appendix B. Internet Transition Considerations

To enhance a large communication system like the Internet, it is important to minimize the disturbance to the existing equipment and processes due to any required modification. The basic EzIP plan is to confine all actionable enhancements within the new SPR module(s). The following outlines the considerations for supporting the transition from the current Internet to the one enhanced by the EzIP technique.

B.1. EzIP Implementation

B.1.1. Introductory Phase

A. Insert an SPR in front of a web-server that desires to have additional subnet addresses for offering diversified activities. This configuration is commonly referred to as a reverse proxy. For the long term, a new web server may be designed with these two functional modules combined.

. The first address of a private network address pool, e.g., 242.0.0.0, used by the SPR should be reserved as a DMZ channel directing the initial incoming service requesting packets to the existing web server. This will maintain the same current operation behavior projected to the general public.

. The additional addresses, up to 255.255.255.255 may be used for EzIP address extension purposes. Each may be assigned to an additional web server representing one of the business’s new activities. Each of these new servers will then respond with EzIP header to messages forwarded from the main server, or be directly accessible through its own EzIP address.

B. Insert an SPR in front of a group of subscribers who are to be served with the EzIP capability. The basic service provided by this SPR will be the CG-NAT equivalent function. This will maintain the same current baseline user experience in accessing the Internet.

C. Session initiating packets with basic IPv4 header will be routed by SPRs to a business’s existing server at the currently published IPv4 public address (discoverable through existing DNS). The server should respond with the basic IPv4 format as well. Essentially, this maintains the existing user experience between a customer and a web server within an EzIP-unaware environment.

So far, neither the web-server nor any subscriber’s IoTs needs to be enhanced, because the operations remain pretty much the same as

today’s common practice utilizing CG-NAT assisted connectivity. See Appendix A.1. for an example.

D. Upon connection to the main web server, if a customer intentionally selects one of the new services, the main web server should ask the customer to confirm the selection.

. If confirmed, implying that the customer is aware of the fact that his IoT is being served by an SPR, the web server forwards the request to a branch server for carrying on the session via an EzIP address.

. The SPR on the customer side, recognizing the EzIP header from the branch web-server, replaces the CG-NAT service with the EzIP routing.

. For all subsequent packets exchanged, the EzIP headers will be used in both directions. This will speed up the transmission throughput performance for the rest of the session. See Appendix A.2. for an example.

B.1.2. New IoT Operation Modes

A. EzIP-capable IoT will create EzIP header in initiating a session, to directly reach a specific EzIP-capable web-server, instead of the manual interaction steps of going through the DMZ port then making the selection from the main web server. This will speed up the initial handshake process. See Appendix A.2. for an example.

B. To communicate with an EzIP-unaware IoT, an EzIP-capable IoT should purposely initiate a session with conventional IP header. This will signal the SPRs to provide just the CG-NAT type of connection service. See Appendix A.1. for an example.

B.1.3. End-to-End Operation

Once EzIP-capable IoTs become wide spread among the general public, direct communication between any pair of such IoTs will be achievable. An EzIP-capable IoT, knowing the other IoT’s full EzIP address, may initiate a session by creating an EzIP header that directs SPRs to provide EzIP service, bypassing the CG-NAT process. See Appendix A.2. for an example.

B.2. SPR Operation Logic

To support the above scenarios, the SPR should be designed with the following decision process:

B.2.1. Sending an IP packet out for an IoT or an RG

If the IP header contains EzIP Option word, SPR will route it forward by using the EzIP mechanism (replacing Source Host Number by SPR's own and filling in Extended Source No. if not already there). Otherwise, the SPR provides the CG-NAT service (assigning TCP Source Port number and allowing the packet to masquerade with the SPR's own IP address, plus creating an entry to the state (port-forward / look-up / hash) table in anticipation of the reply packet).

B.2.2. Receiving an IP packet from the ER

If a received IP packet includes a valid EzIP Option word, SPR will provide the EzIP routing service (utilizing the Extended Destination No. as the Destination Host Number). If only Destination Port number is present, CG-NAT service will be provided. For a packet with plain IP header (with neither EzIP nor CG-NAT information), it will be dropped.

B.3. RG Enhancement

With IPv4 address pool expanded by the EzIP schemes, there will be sufficient publicly assignable addresses for IoTs wishing to be directly accessible from the Internet. On the other hand, the existing private networks may continue their current behavior of blocking session-request packets from the Internet. In-between, another connection mode is possible. The following describes such an option in the context of the existing RG operation conventions.

B.3.1. Initiating Session request for an IoT

Without regard to whether the IP header is a conventional type or an EzIP one, a RG allows a packet to masquerade with the RG's own IP address by assigning a TCP port number to the packet and creating an entry to the state (port-forward / look-up / hash) table. This is the same as the current RG-NAT practice.

B.3.2. Receiving a packet from the SPR

The "Destination Port" value in the packet is examined:

A. If it matches with an entry in the RG-NAT's state-table, the packet is forwarded to the corresponding address. This is the same as the normal RG-NAT processes in a conventional RG.

B. If it matches with the IP address of an active IoT on the private network, the packet is assigned with a TCP port number and then forwarded to that IoT.

Note that there is certain amount of increased security risk with this added last step, because a match between a guessed destination identity and either of the above two lists could happen by chance. To address this issue, the following proactive mechanism should be incorporated in parallel:

C. If the "Destination Port" number is null or matches with neither of the above two lists, the packet is dropped and an alarm state is activated to monitor for possible ill-intended follow-up attempts. A defensive mechanism should be triggered when the number of failed attempts has exceeded the preset threshold within a predetermined finite time interval.

In brief, if the IP header of a session requesting packet indicates that the sender knows the identity of the desired destination IoT on a private network, the common RG screening process will be bypassed. This facilitates the direct end-to-end connection, even in the presence of the RG-NAT. Note that this process is very much the same as the AA (Automated Attendant) capability in a PABX telephone switching system that automatically makes the connection for a caller who indicates (via proper secondary dialing or an equivalent means) knowing the extension number of the destination party. Such process effectively screens out most of the unwanted callers while serving the acquaintance expeditiously.

Appendix C. EzIP Realizability

The EzIP scheme proposes a new type of network router, called SPR, capable of utilizing 240/4 address transported via the Option word mechanism in the EzIP Header. In particular, EzIP may optimally be first deployed in the form of a Regional Area Network (RAN) wherever desired. Each RAN starts from one IPv4 public address to serve up to 256M IoTs or premises. For such a configuration, an SPR will operate with the degenerated EzIP Header which is identical to the basic IPv4 Header, except the addresses are from the 240/4 netblock. Since this can be accomplished by simply expanding the scope of the accessible address pool within the IPv4 protocol, there is hardly any need to modify the design of existing routers.

Having been "Reserved for Future Use" for so long (since 1981-09), however, it is a challenge to identify current equipment that may be conducive to the use of the 240/4 netblock. Un-documented behaviors, observed through extensive research and testing of products in-use and on-the-market as well as public domain firmware, confirm that certain pairs of router and IoT / PC OS are already partially supporting this mode of operation. This unexpected discovery sets the baseline for the following interim report.

C.1. 240/4 Netblock Capable IoTs

A. Open source Xubuntu OS (V.18.04.1) enables a PC to assume both dynamic and static IP addresses, through the same physical Ethernet port, simultaneously. The former operates in the default DHCP client mode with conventional three private netblocks, while the latter accepts manually set static addresses including those from the 240/4 netblock. Making use of this "dual personality", connectivity between two similarly equipped PCs can be established first through a compatible router (described in the next subsection) by "ping"ing each other with the dynamic address. Using the static 240/4 addresses, the additional networking channel through the same router can then be confirmed.

B. Several other PC OSs, such as Chrome (V.74.0.3729.125), LinuxMint V.19 tara (Ubuntu V.4.15.0), Mojave (OSX 10.14.1) and Ubuntu 19.04 (Ubuntu 5.0.0), have been found to behave similarly, although partially and not as conveniently.

C.2. 240/4 Netblock Capable Routers

A. Open-source router firmware OpenWrt (V18.06.1) currently does not utilize the 240/4 netblock in its DHCP operation, while it would not reject the process of specifying such but would not function

properly afterwards. Yet, it transports, in its native configuration, 240/4 addressed "ping" packets between two 240/4 capable PCs anyway.

B. Also, a common RG, TP-Link Archer C20 AC750 (F/W V4_170222 / 0.9.13.16 v0348.0) rejects setting its DHCP pool to use the 240/4 netblock, but transports 240/4 addressed "ping" packets, nonetheless.

C. Similarly, Verizon FiOS-G1100 RG (H/W: 1.03, F/W: 02.02.00.14 UI Ver: v1.0.388) will not allow its DHCP server to utilize the 240/4 netblock, but transports the 240/4 addressed "ping" packets, just fine.

D. Other routers, such as LinkSys E3000 (DD-WRT v24-sp2 (05/27/13) mini (SVN Rev. 21676), have been found to exhibit similar behavior.

E. Furthermore, test data suggest that 240/4 addressed "ping" and "traceroute" packets from some of the above setups could have propagated through an IAP’s ER (108.30.229.xxx, Verizon’s Edge Router) into the Internet. The addresses (130.81.171.xxx) that they arrived at appear to be Verizon’s internal routers. If these are not CRs (Core Routers), at least they are ARs (Aggregate Routers).

C.3. Enhancing an RG

The above observations suggest that Xubuntu OS based PCs are likely ready to network as 240/4 addressed DHCP clients. To complement this capability, we need a router that can function as a 240/4 DHCP server. Although the OpenWrt firmware appears to be closer to this desired functionality than the TP-Link Router, the source code of the latter being hardware specific would better facilitate the firmware enhancement efforts. Accordingly, the following outlines the steps being planned to bring TP-Link Router and Xubuntu OS based PCs up to a state for performing the essential SPR functions:

C.3.1. Enhance the TP-Link Router firmware to include the 240/4 netblock in its DHCP pool.

C.3.2. Verify that Xubuntu OS based PCs will accept 240/4 based DHCP assignment from the enhanced Router above. With this, deactivate the static address settings in the PCs.

C.3.3. Send 240/4 destined traffic between two Xubuntu PCs to be sure that it is transported through the Router. Three tests will be conducted; sending "ping" and "traceroute" packets to confirm the

basic connectivity as well as file transfer to verify TCP/IP capability.

C.3.4. A separate second TP-Link Router will then be plugged into this first Router as a client IoT to verify that it would accept a 240/4 address as its WAN port designation. Based on this, the second Router will serve as an RG providing the conventional private network environment (10/8, 172.16/12 and 192.168/16 netblocks) to common IoTs, allowing them to continue their current operations without modification, at all.

C.4. SPR Reference Design

The above pair of enhanced Routers can be used as the SPR model for enhancing industrial grade routers that are capable of the daily traffic level expected by a RAN.

Note that including 240/4 netblock in the DHCP pool for the LAN of the first Router and accepting the 240/4 address assignment on the WAN port of the second Router are two orthogonal capabilities. They can be implemented in the same physical Router, consolidating both modifications into one single SPR module.

C.5. RAN Deployment Model

The above SPR reference design is essentially an existing common IPv4 RG with two simple enhancements:

I. Upstream (WAN) port capable of being a DHCP client accepting 240/4 address assignment, in addition to the ordinary IPv4 public address.

II. Downstream (LAN) port providing DHCP service to client IoTs using the 240/4 netblock, in addition to the three conventional private netblocks.

By selectively activating these capabilities, three versions of SPRs can be derived for completing a functional RAN model:

C.5.1. Root / Gateway SPR:

This is the first SPR for starting a RAN from an IPv4 public address. As such, the upstream port of this SPR should accept a public IPv4 address. And, its downstream port will use the 240/4 netblock in its DHCP pool.

Note that this particular type of SPR is only needed for a RAN demonstration setup. In an actual RAN deployment, a proxy gateway that caches the Internet traffic for improving the operation efficiency will naturally perform the same function of this Root SPR, by virtue of being a more capable two-port device.

C.5.2. Intermediate SPRs:

To optimize the performance requirements on the routing processor, a practical SPR is not expected to handle all 256M IoTs in a single module. A RAN should have several layers of SPRs in a tree structure, each handles a subset of the 240/4 netblock. This architecture enables processing local traffic locally. Only communications with distance parties need be consolidated by going through the higher layers of SPRs for delivery. For this type of SPRs, both their upstream DHCP client port and downstream DHCP Server pool will operate on sub-240/4 netblocks, segregated according to the numbering plan in the RAN system design.

C.5.3. RG SPR:

To serve existing IoTs on customer premises, this SPR will be configured to accept a 240/4 address on its upstream port, while the downstream port assigns addresses from the three conventional private netblocks of RFC1918 to its DHCP client IoTs.

Appendix D. Enhancement of a Commercial RG

Since the 240/4 netblock is just one part of the full IPv4 address pool, there is nothing special about it. In principle, all we need to do to utilize it is to include it within the usable ranges of a router's addresses. However, perhaps because it has been reserved for so long, hardly anyone has been paying attention to how the 240/4 netblock has been treated in current router programs. An intuitive assumption is that there may be a database that lists all acceptable address ranges or netblocks. If so, the EzIP enhancement would entail adding the 240/4 netblock to the list. On the other hand, the current approach maybe is based on singling out specific unusable IP addresses. Then, eliminating such process is sufficient. It turns out that a commercial RG product appears to be operating with the latter approach. From such, the task would become simply commenting out the program statements that are rejecting the 240/4 netblock.

D.1. Candidate Code for Modification

The following short JavaScript function named "ifip" in the TP-Link Archer C20 V4 source code has been shown to selectively reject specific ranges of IP addresses. In particular, Line 1047 uses a "2's Complement" technique to identify the 240/4 netblock as "PRESERVED", thus rejecting it. A quick scan of the firmware code in the router indicates that this function is a popular utility because there are numerous processes calling for it. So, this should be the best candidate to start testing our concept.

```
   lib.js:1040:ifip: function(ip, unalert) {
   lib.js-1041-if ((ip = $.ip2num(ip)) === false) return
$.alert(ERR_IP_FORMAT, unalert);
   lib.js-1042-if (ip == -1) return $.alert(ERR_IP_BROADCAST,
unalert);
   lib.js-1043-var net = ip >> 24;
   lib.js-1044-if (net == 0) return $.alert(ERR_IP_SUBNETA_NET_0,
unalert);
   lib.js-1045-if (net == 127) return $.alert(ERR_IP_LOOPBACK,
unalert);
   lib.js-1046-if (net >= -32 && net < -16) return
$.alert(ERR_IP_MULTICAST, unalert);
   lib.js-1047-if (net >= -16 && net < 0) return
$.alert(ERR_IP_PRESERVED, unalert);
   lib.js-1048-return 0;
   lib.js-1049-},
```

D.2. Proposed Modification

To stop rejecting the 240/4 netblock addressed packets, below is a modification that comments out Line 1047, a modification that has been shown to eliminate JavaScript pre-validation of 240/4 IP addresses, allowing them to be sent within the router, where a second layer of validation rejects them in a different way.

```
   lib.js:1040:   ifip: function(ip, unalert) {
   lib.js-1041- if ((ip = $.ip2num(ip)) === false) return
$.alert(ERR_IP_FORMAT, unalert);
   lib.js-1042- if (ip == -1) return $.alert(ERR_IP_BROADCAST,
unalert);
   lib.js-1043-   var net = ip >> 24;
   lib.js-1044- if (net == 0) return $.alert(ERR_IP_SUBNETA_NET_0,
unalert);
   lib.js-1045- if (net == 127) return $.alert(ERR_IP_LOOPBACK,
unalert);
   lib.js-1046- if (net >= -32 && net < -16) return
$.alert(ERR_IP_MULTICAST, unalert);
   lib.js-1047- //if (net >= -16 && net < 0) return
$.alert(ERR_IP_PRESERVED, unalert);
   lib.js-1048- return 0;
   lib.js-1049-},
```

D.3. Performance Verification

Initially, the TP-Link Archer C20 router’s GPL source code package from the manufacturer would not go through compilation process. A revised version allowed us to build a firmware file. Yet, it failed in loading into the hardware. Interactions continue with the manufacturer hoping to resolve this basic issue soon. Unfortunately, this issue remains pending to this day.

Appendix E. Utilizing Open-Source Router Code

An alternative to the above is to make use of open-source router codes for the EzIP implementation. The advantage of this approach is that once it is verified in one commercial router, interested parties may then load the same vintage of open-source codes to their own preferred routers for replicating the operation. The challenge to this approach, however, is that open-source codes are "generic" for supporting a wide range of brands and models. Customization must be made to adapt it for a specific router model to generate an executable binary file for the target device as its firmware. As well, this configuration information will be needed each time the source code is modified for a new application, such as the EzIP. Interestingly, such knowledge appeared to be not in an "open" document. In the process of studying such, we discovered that OpenWrt was planning to enhance its Linux core which included the removal of the current restriction on using 240/4. Although their intention was to be able to use the 240/4 pool as the fourth private netblock, such capability suited our EzIP scheme just fine. So, we waited for the release of the OpenWrt 19.07 and further for its more stable OpenWrt 19.07.2 version, before attempting the EzIP application. Below is a WIP report of our test results based on OpenWrt 19.07.3.

E.1. EzIP Realizability Test Bed

The first step is to create a LAN environment served by a router utilizing the 240/4 netblock. Upon loaded OpenWrt 19.07.3 into a commercial TP-Link Archer C20 V4 Router, it operated with 240/4 address pool as if it was the fourth private netblock. IoTs capable of utilizing 240/4 netblock operated fine under this environment. Specifics of this effort is reported on Page 2 of the following whitepaper:

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

E.2. RAN Architecture Demonstration

The goal of a RAN Demo is to transport a conventional IPv4 (public) netblock addressed IP packet though a 240/4 environment and then back to an IPv4 private network operating with one of the three conventional netblocks (10/8, 172.16/12 or 192.168/16). This process will increase the assignable addresses, while allowing all IoTs to retain their existing operation characteristics. To simulate such a RAN, we need a RG that can operate as a client in the 240/4 environment established by Appendix E.1. above, while maintaining

its DHCP LAN service to a conventional private network. It has been identified that besides OpenWrt 19.07.3 supported routers, at least one RG (Sagemcom RAC2V1S) provided by Spectrum cable service delivers this function. Page 4 of the above whitepaper details the configuration and operation of such a RAN. In addition, during past experiments, RG for Verizon’s FiOS service was found to be already transporting 240/4 addressed packets, as well. Combined, this means that most of existing private networks may continue normal operations under the inserted RAN environment while the latter provides assignable 240/4 addresses to additional premises for expanding the system capacity.

E.3. EzIP Compatible Routers

At the last count, there were 478 branded router models supported by OpenWrt 22.03.5. In fact, it turns out that for an existing IPv4 router to become an SPR for supporting the EzIP operation, all needs be done is "disabling the existing program code that has been disabling the use of the 240/4 netblock". Such effort is expected to be rather minimal for parties having control of the relevant program source codes. Consequently, most existing IPv4 routers should be able to support EzIP through finite enhancement processes, even if they are currently not supported by OpenWrt 19.07.3 (or newer).

Appendix F. Sub-Internet

Since each RAN serving up to 256M IoTs can be operated with just one IPv4 address for interacting with the Internet, it follows that if a buffering device is inserted in line between the two for relaying requests to the Internet and caching the responses from the Internet, a RAN could behave like a pseudo (although miniature) Internet from its clients' perspective for practical purposes. Such buffering function may be provided by a Gateway module which is commonly used by institutions for serving their respective LANs. Terminology wise, this Gateway is called Transparent / Intercepting Proxy as compared to other forms of cache proxies such as Peer Proxy, Reverse Proxy, etc. Combining a RAN with a Gateway, a Sub-Internet is formed that can operate as a stand-alone module to provide Internet services. Below is a brief description of a Gateway for serving a RAN.

F.1. Gateway Configuration

Besides the above-mentioned caching functions, a Gateway, being a two-port device, can also bridge two different netblocks together. This is convenient because the Gateway's upstream port uses the conventional public IPv4 address while the downstream port supports the RAN that runs on 240/4 netblock. However, this is not a necessity, because the root SPR in the RAN is configured, by default, as a DHCP client so that it can work from either netblock, anyway.

F.2. Gateway Setup

A Raspberry Pi4 single board computer loaded with Raspaian Buster Linux for Pi4 OS is used as the base for running a cache proxy (squid/oldstable,now 4.6-1+deb10u6 armhf) to serve as a Transparent Proxy.

F.3. Sub-Internet Operation

Several basic functions, such as web access, file transfer, eMail, etc. are being tested. Initial results are encouraging. The WIP (Work In Progress) file posted at the following URL has been updated to report the latest results of the ongoing efforts.

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

Appendix G. Discussions

The work reported here originated from studying the IPv4 Address pool depletion event. The outcome, however, threaded through a few other Internet aspects. These unexpected intertwining implications made presenting the EzIP proposal challenging. In this Appendix, several identifiable topics are outlined to coordinate discussions that otherwise might diverge.

G.1. Activation of EzIP Capability

The primary action item of the EzIP proposal is to make use of the long-reserved 240/4 netblock, efficiently.

A. Since the 240/4 netblock was reserved from the overall IPv4 address pool through administrative decisions, there was no specific technical reason that made it unique or incompatible with any existing networking hardware. However, after years of intentionally not using it, most products do appear not supporting 240/4 at the first glance.

B. The basic approach for utilizing the 240/4 netblock is disabling the program code in the networking equipment that has been disabling the use of the 240/4 netblock. The actual implementations may vary depending on how the target equipment was originally designed. However, the "IPv4 Unicast Extensions Project" reported that most networking products and operating systems examined were already supporting 240/4 in various unpublicized applications. Or, they may be enhanced by a minor program modification. For example, there is at least one program that could be enhanced by simply commenting out one line in its code that has been blocking 240/4 addressed packets. These experiences can be used as benchmarks for reviewing other candidates.

G.2. EzIP Network Architecture

The ultimate goal of EzIP is to make the Internet a full-fledged worldwide communications backbone, providing end-to-end connectivity between any pair of customer premises, including IoTs directly connected to the Internet. However, such service is currently not in demand, because server-client model is commonly used today. To begin a seamless transition from the existing Internet configuration, the EzIP building block RAN utilizing the degenerated EzIP header will be deployed first.

A. To avoid perturbing daily operations, the starting point of the EzIP deployment is to expand the Internet architecture without

affecting the existing setups. This can be achieved by treating the 240/4 as the second netblock under RFC6598, so that 240/4 addresses may be reused by SPRs in geographically disjoint areas to avoid one SPR cluster from interfering another, or Internet core routers.

B. Due to the size of the 240/4 netblock, each SPR cluster can serve significantly more subscribers than one 100.64/10 netblock is capable of. Consequently, several CG-NAT clusters may be consolidated into one 240/4 netblock, freeing up public IPv4 addresses.

C. With these characteristics, RANs can be established. Each can be viewed as a hoovering kite tethered from the Internet core via an umbilical cord made of one IPv4 public address. Consequently, RANs can be operated independently of one another as well as the Internet core. They only communicate through the umbilical cords when information exchange is needed.

D. As long as the packets transported through the umbilical cords conform to IPv4 protocols and conventions, each RAN has the freedom of choosing transmission technologies, routing schemes, operation disciplines, business practices, etc. for activities within itself.

E. As RANs grow and expand, routers may be deployed between RANs for transporting packets directly as the traffic volume dictates. These enable the hoovering kites to be knitted together, eventually forming a complete spherical overlay network in parallel to the existing Internet. The two may operate independently, except exchanging information when needed. This configuration offers subscribers the choice of using either network, or even simultaneously to experiment with both for comparison.

G.3. EzIP Deployment Vehicles

To focus on presenting the EzIP concepts, SPR (Semi-Public/Private Router) is introduced. In reality, such routers are already being used in the field. Only minor program upgrade is needed for enabling them to perform the SPR functions.

A. CG-NAT (Carrier Grade Network Address Translation): The proposed EzIP network (the RAN) has the same architecture as that for the CG-NAT. The only difference is the size of the netblocks used. To start deploying EzIP, all need be done is to enable the existing CG-NAT routers to handle the 240/4 netblock. The lowest level CG-NAT router may start first by assigning 240/4 addresses to customer premises and begins routing packets within itself utilizing the 240/4 in the native IPv4 header address fields. This transition can be kept

local, finite and transparent from others by maintaining the current NAT behaviors for interfacing with neighboring routers.

B. The above process can propagate to peer and upstream routers in the CG-NAT architecture until reaching the root router that is connected to the Internet core via the umbilical IPv4 public address. At such point, the transition of one CG-NAT cluster to a RAN is complete.

C. CDN (Content Delivery Network): This currently predominant Internet business model meshes well with the CG-NAT. Thus, CDN can be similarly enhanced to take advantage of the EzIP characteristics.

D. CDN’s distributed data centers also conveniently provide the RAN gateway functions, such as store and forward traffic, address translation between the 240/4 used in RAN and the public IPv4 used in the Internet core.

G.4. 240/4 Address Administration

The limited IPv4 address pool size necessitated the current dynamic nature of Internet practice. It is not an optimal approach because it introduces unnecessary operational complexity that degrades the system robustness. Whenever possible, we should navigate away from such.

A. The size of the 240/4 netblock enables static address assignment. It follows that addresses can be deterministically correlated to geographical locations of the customer premises at the resolution level desired.

B. In addition, hierarchical address administration within each RAN can be practiced, further simplifying operation logistics.

G.5. Routing Strategy

The above recommended static address assignment facilitates hierarchical routing. This should be regarded as an enhancement to, but not a replacement of, the current mesh routing practice.

A. By default, routing within the EzIP environment should normally use hierarchical process for more reliable and efficient performance.

B. Dynamically built routing table by detecting nearby router announcements should continue its operation, but serving as a backup to the default.

G.6. Network Robustness

While EzIP scheme itself had no notion about cyber security considerations, its deterministic properties, such as static addressing and hierarchical routing, do reduce the vulnerability of the current dynamic approach which has been exploited by perpetrators due to its weak support to real time traceability and forensic analysis.

G.7. Cost

The initial EzIP deployment is via enhancing programs in existing CG-NAT routers. So, minimal cost is expected. For service growth in the future, new hardware capable of IPv4 only is sufficient. They should cost the same as, if not less than, those also capable of IPv6.

G.8. Redundancy

Each RAN is described as having hierarchical routing as well as one public IPv4 address to the Internet core. These are just the fundamental capabilities. They do not prevent a RAN from having multiple traffic channels within itself, to the Internet core, or direct connections to other RANs for mesh routing, load balancing, etc. considerations.

Appendix H. Manifestations and Implications

The below list summarizes discrete topics that relate to the EzIP proposal in various respects.

A. After resolving the assignable IPv4 public address pool exhaustion issue, EzIP still has much more spares in reserve.

B. EzIP initial deployment relies only on activating the use of the long-reserved 240/4 netblock,

C. Maintaining the current Internet architecture, and

D. Utilizing the CG-NAT routers as the deployment vehicles. So that their NAT mode of operation will coexist, or can be phased out, if desired.

E. Many RGs (Routing / Residential Gateway) are already able to operate as DHCP clients on 240/4 networks. For example, a long list of RGs may be enhanced by loading with the latest OpenWrt code.

F. Consequently, IoTs on private premises do not need be enhanced to be 240/4 compatible. This also means that OSs such as Windows are no longer a concern for the first (primary) phase of EzIP deployment.

G. EzIP can achieve its long-term end-to-end connectivity goal by simply relying upon RFC791.

H. EzIP does not perturb the current Internet architecture. Instead, EzIP enhances it with an expansion network operating in a newly defined overlay cyberspace.

I. EzIP is compatible with all up-to-date IPv4 hardware, without requiring any IPv6 related capability.

J. Un-perturbed by EzIP, the Internet core regards RAN as a private network, allowing independent operations within each RAN. This offers practical test beds for end-users to participate in experimenting new techniques and issues that, up until now, there has not been such a public facility.

K. On the other hand, while coexisting with the Internet core, RANs can build up their own network to be an overlay to the former.

L. In summary, the EzIP proposal essentially creates a 64-bit (capable of even longer) addressed spherical overlay communication

architecture in two finite steps by utilizing the IPv4 reserved resources (240/4 netblock) and rudimentary protocol (RFC791). The resultant network is in parallel to, while can be independent of, the current global Internet. Neither IoTs nor Internet core need be modified for the initial phase of the EzIP deployment to resolve the IPv4 address shortage issue. In the long term, only those wishing to have the full end-to-end communication will need to use enhanced, or new IoTs that are capable of handling 240/4 address.

Appendix I. Miscellaneous Considerations

Through recent online discussions, it became apparent that more than a few readers were distracted by the fact that certain topics of particular interest to some readers were not dealt with in this document. Consequently, a reader might get an impression that the EzIP would not handle such a situation properly. Below is a digest based on such interactions in an attempt to clarify those concerns.

A. First of all, although quite a few areas of the Internet may eventually be affected, EzIP is not proposing a new system out right, but starts from incrementally enhancing an existing operation through systems engineering efforts. That is, this proposal initially focuses only on specific Internet aspects to be changed or improved, such as numbering plan and its related administration, etc. It should be understood that other unmentioned conventions, practices, etc. are to remain unperturbed, at least during the initial EzIP deployment phase. This is to assure a smooth transition.

B. The activation of 240/4 netblock requires disabling the networking program codes that have been disabling the use of the 240/4 netblock. After many years of in reserve, how was this portion of the process actually being implemented became hidden from most people. It turns out that there exists at least one instance that this can be done by simply commenting out one line of the existing program code. Although this does not mean that every such task is trivial, this example should be regarded as an inspiration for reviewing and enhancing equivalent programs that are more complex. Since the use of 240/4 can be confined locally within a router, one at a time, without affecting the neighboring ones, this should be an encouraging starting point to get simpler programs updated first while working on more involved ones.

C. The key action item proposed by the EzIP scheme is to utilize the long-reserved 240/4 netblock for use in parallel to the 100.64/10 netblock so that the CG-NAT operation can be streamlined. Through this process, there are several implied considerations. For example:

a. Since the size of the 240/4 is 64 times of the 100.64/10, each block of the former is sufficient to serve a much larger geographical area than the latter could. There is no longer any need to dynamically reuse addresses within a CG-NAT cluster as under RFC6598, up to a full RAN. That is, the 240/4 netblock may be administrated as a globally reusable address pool for each RAN within a finite geographical area.

b. With more than sufficient addresses to assign for each RAN, 240/4 addresses may be assigned statically. This streamlines the administration which improves the network robustness against cyber intrusion.

c. Static addresses are ideal for associating with geophysical locations of subscribers to simplify bookkeeping as well as operations. It follows that the 240/4 addresses should be regarded as shared natural resources that respective local jurisdictions are responsible for managing, instead of private properties handled by global organizations with financial considerations.

d. Prioritize the use of IP addresses for purely "location" identification instead of "application" related purposes will significantly preserve the availability of the address pool.

D. EzIP initial deployment starts from Internet Edge Routers (ER - the lowest level closest to subscribers) whose root ports should retain the existing IP addresses assigned by the next higher up routers. With NAT function still operational, no other routers could sense that this particular router has upgraded to using the 240/4 netblock, thus avoiding the interoperability issues. This process can progress up the router chains wherever possible until all routers of the entire area are using the 240/4 netblock. Even so, the whole RAN still appears to the Internet core as the original CG-NAT cluster. Consequently, the EzIP’s initial deployment phase may be regarded as stealthy. A RIPE Labs article reported that enterprises, such as Amazon, Vodafone, Adobe, Verizon, etc. have been using 240/4 unannounced. This validated the basic scheme proposed in this draft. On the other hand, it also sounded the alarm of potential confusions and conflicts if the 240/4 netblock continued to be left in the current "reserved" state without clear purpose.

https://labs.ripe.net/author/qasim-lone/2404-as-seen-by-ripe-atlas/

E. The procedure as described above will not affect the existing DHCP related practices. Since geographical correlated numbering plan does not work against the DHCP, it would be advisable to do so ASAP, in preparation for a more concise overall operation.

F. Architecture wise, each RAN needs one IPv4 address for the interface with the Internet core. This does not preclude a RAN from having multiple IPv4 addresses and physical channels for traffic optimizations such as load balancing, redundancy, reliability, etc.

G. As well, static address assignment recommended here facilitates the hierarchical routing for efficiency. However, it does not prevent continuing the existing meshed routing practices, or the mixed use of either. The priority between the two may be determined pending on reviews of the relative merits.

H. Each RAN appears to be a private network to the Internet core. It may be viewed as a kite flying in the sky tethered through one IPv4 address based umbilical cord. Collectively, RANs form a continuous layer of networking fabric wrapped around the entire current Internet core to become an overlaying Sub-Internet. This configuration is achieved by having CG-NAT clusters enhanced to RAN incrementally, then inter-connected where possible, while not requiring any abrupt step-wise changes across the board. Consequently, the Sub-Internet is architecturally parallel to, but operationally independent of the existing Internet core.

I. When considering the use of a new address block, the question of whether the existing environment would support it naturally comes up. It has been a common belief that most existing networking devices drop packets with 240/4 addressing. On the other hand, there are reports, such as work conducted by "IPv4 Unicast Extension Project", stating evidences of the contrary. Below is a summary of the current status from the EzIP deployment perspective:

a. RG (Routing / Residential Gateway): The open source OpenWrt project has a long list of brand-named RG models supporting 240/4 addressing. With this, private premises are buffered from 240/4 addressing. That is, none of the IoTs on private networks will sense any changes. They can continue operating with private netblocks under RFC1918.

https://openwrt.org/toh/start

b. Since EzIP deployment is incrementally from the bottom of the network up, universal availability of this facility is not required immediately. Instead, EzIP compatible routers can seek one another to gradually link up for forming a RAN. Those routers unable to support EzIP operation will be left out of the RAN configuration. Where this occurs, OpenWrt also supports Edge Routers (ER) from Ubiquiti Networks and D-Link that may fill the gap.

c. For Aggregate Routers (AR) and above, at least one Network Operating System (NOS) "White Box" vendor confirmed that they would be ready to provide products supporting 240/4 operation if customers ask for it.

d. During the initial phase, Core Routers (CR) do not need be enhanced to support EzIP, because all RANs are tethered thru IPv4 addresses as if they were conventional private networks. Even upon the use of the Option Word mechanism for end-to-end connectivity, a CR does not need any change as long as it is not programmed to drop packets with Option Word.

J. The full EzIP header utilizing Option Word mechanism reported in the main body of this Draft will not be needed for the initial EzIP deployment phase. Such mechanism will only be activated for those subscribers who wish to have direct (end-to-end) communication, e.g., exchanging private personal eMails. Since the current Internet cannot provide such service, this capability should be treated as an optional premium service in the future. It should only be considered after the basic EzIP deployment of enhancing the CG-NAT operation is completed.

K. In summary, starting from one IPv4 public address, EzIP makes use of 240/4 to establish private networks which expands CG-NAT clusters to serve a larger area forming isolated RANs. When areas encompassed by RAN grow bigger and become adjacent with one another, the Sub-Internet is formed which is an overlay network enveloping the current Internet. It is envisioned that each of these steps will be incremental with minimum perturbation to the existing operations.

Appendix J. Streamline The Internet

EzIP can be viewed as an incremental enhancement to the Internet via applying the novel use of a block of IPv4 addresses over one or more existing CG-NAT facilities. In doing so, much of the current operations may be kept intact while the additional capabilities are implemented to establish an overlay network, called RAN. Since the 240/4 netblock has been in the "Reserved" status for so long, however, it may take some efforts to ready the related components for boot-strapping up this new configuration. This Appendix outlines the considerations for such transition utilizing minimum instrumentation.

J.1. Enhancing the existing facility

a. Although EzIP proposes to utilize the 240/4 netblock, one of its primary goals is to expedite the transition by avoiding to impose such on IoTs because the impossible task of upgrading the huge quantity of IoTs already in the field. On the other hand, to verify building block capabilities and network operations, a pair of IoTs capable of transmission tests (sending and receiving 240/4 addressed packets) is needed. Instead of industrial grade test instruments, common portable PCs capable of this function would be preferred for encouraging the public participation in this deployment. It is known that Windows-OS based PCs are uncapable of this task, while Linux-OS does support. In particular, Xubuntu V18.04.1 was found to be most convenient because it can simultaneously assume dual IP addresses. That is, each such PC can operate with two IP addresses, one functions as a DHCP client on a conventional IPv4 network, while the second behaves like an IoT with static 240/4 address. The former establishes the physical connectivity between two points through a conventional IPv4 network. Then, the latter verifies the transmission path between the same two via a 240/4 addressed packet over the same physical medium.

https://xubuntu.org/

This enables the same pair of notebook PCs to be used at various locations of any network with conventional IPv4 ranges, 240/4 netblock, or combined, back and forth, without the need to change any configuration setting, nor to reboot the PCs.

b. With all on-premises IoTs remaining on RFC1918 netblocks, an RG (Routing/ Residential Gateway) does not need to modify its down-stream (LAN) side, except being able to operate as a 240/4 DHCP client on the up-stream (WAN) side. Many off-the-shelf RGs are already capable of this, although not explicitly stated in their

specifications. To assure a definitive starting base, any device on the below long list of commercial RGs may be made fully 240/4 capable by replacing its firmware with OpenWrt V19.07.3 or later.

https://openwrt.org/toh/start

c. Basic instrumentation: A pair of Xubuntu based notebook PCs and any one of the OpenWrt based RGs as described above can form a simple test bed for verifying a network device's functionality as a client, a server or both in a 240/4 environment.

d. For network routers, IPv4 Unicast Extension Project reported that many Linux based routers have been capable of supporting 240/4. In addition, one of OpenWrt supported D-Link smart managed switch DGS-1210-28 may serve as a basic building block to initiate deploying the RAN fabric.

https://us.dlink.com/en/products/dgs-1210-28-28-port-gigabit-smart-managed-switch

e. With these, a Regional Area Network (RAN) Simulator may be set up to begin experimenting RAN operations.

https://www.avinta.com/gallery/RegionalAreaNetworkSimulator.pdf

f. As suggested by page 5 of the above, an entire RAN, limited only by the number of static addresses available from one 240/4 netblock, could be served by the smart switches operating at L3 (Level 3). This configuration removes the need for dynamic protocols such as DHCP. DNS, AS and BGP (Border Gateway Protocol), making RAN operations concise and deterministic to establish a robust infrastructure for improved cyber security.

J.2. Address administration

a. With the large (256M) address pool, each 240/4 netblock is sufficient to support a sizable population. For example, assuming one stationary and one mobile IP address per capita, most geographic regions and political territories with population up to 128M can be served by just one RAN. This enables the static IP address-based assignment and operations at the entire country level for most.

b. Based on static address having Geolocation property, RAN can operate from an electronic look-up table that only needs be periodically updated through a restricted access. Operating as a plain router without DHCP nor DNS services, CG-NAT protocol is not

needed in an RAN either. Consequentially, an RAN is much less vulnerable to cyber intrusions than a CG-NAT.

J.3. Intra-RAN networking and routing

Within each RAN, IAPs (Internet Access Providers) collectively operate with the IP addresses already assigned to the subscriber premises as one unified network. This avoids each IAP from holding a separate block of allocated addresses for assigning to respective subscribers that creates the need for individual ASes (Autonomous Systems) which in turn requires BGP services for completing a route.

J.4. Communication beyond a RAN

Since RAN appears like an RFC1918 private network to the Internet core, communication between the two can follow the current practices, and using gateway for store and forward services like that in the CDN configuration.

For inter-RAN communications, the full EzIP header format disclosed in the main text will be employed. So that standard Source and Destination Host Numbers are used to transport packets between RANs and the Option Words direct the packet within respective RANs.

J.5. Deployment sequence

a. Since the CG-NAT is an operational facility, the deployment of a RAN can be done incrementally by enhancing network devices from the bottom up in small steps. That is, we can enhance an ER (Edge Router) for assigning static 240/4 addresses to a small community with RGs capable of behaving as 240/4 DHCP clients. This will maintain the current CDN style of services while enabling premises within the community to begin enjoying the individualized peer communication.

b. For ERs that are operating as 240/4 client, NRs (Network Routers) with 240/4 capability may be used to interconnect them, expanding the end-to-end capability to the combined communities served by this NR.

c. Note that as the RAN builds out, it forms an overlaying network that essentially serves the same users as the original CG-NAT fabric, except the routing scheme can be hierarchical. This process may repeat to overlay an entire CG-NAT cluster. Then, several CG-NAT clusters may be combined to from a larger RAN for taking the full advantage of the size of a 240/4 netblock which is 64 fold of that for a 100.64/10 netblock. Eventually, a complete layer of RAN-based

sub-Internet may be formed that overlays on the entire current Internet offering the users the choice of using either or both.

Appendix K. A More Robust Internet

The EzIP network formed by the Appendix J.5.c. process may be viewed from another perspective. There are only around 200 sovereign states around the world, most may be served by one RAN each. Even with some larger states requiring several RANs, a small /22 IPv4 block of 1024 addresses is more than sufficient to identify them all. Applying this as the prefix to respective RANs, the EzIP network becomes a two-tier (or 64-bit) static address system overlaying on the current Internet. Relatively speaking, EzIP is like the traditional PSTN, while CDN is equivalent to broadcasting, such as radio- and cable-based, services. This metaphorical view would facilitate the below analyses.

K.1. A Decentralized Internet

A communication system may have two basic modes of operation, peer-to-peer and master-slave. The traditional PSTN operated primarily with the former, while broadcast services emphasized on the latter.

Now, the Internet is capable of providing both through the same medium by digital technology. Due to the use of dynamic addresses and dominated by the economics for the latter, however, the fundamental essence of the former has been overshadowed. This resulted in the concentration of influence by limited few parties that led to the study of how to decentralize such situation:

https://datatracker.ietf.org/group/dinrg/about/

Since every EzIP subscriber has a worldwide accessible address, direct peer-to-peer global communication becomes natural. This enables the EzIP network to serve as a decentralized infrastructure for whomever needing it. On the other hand, the broadcast modes do not care about which form of address to use. So, its operations are not affected even if they are switched to use static EzIP addresses.

With both modes operational simultaneously based on EzIP, we can then optimize economical tradeoff considerations wherever appropriate.

K.2. A Deterministic Internet

Recent studies identified that the bounded nature of L3 forwarding is a desirable characteristic for improving Internet transmission performance:

https://datatracker.ietf.org/wg/detnet/about/

Based on static addresses, EzIP network inherently operates at L3. It would naturally enable the Internet to establish an environment that is conducive for deterministic services.

K.3. A Secure Internet

Much of the Internet vulnerabilities originated from the dynamic nature of its operations. While necessitated by the earlier IPv4 address pool shortage, they unfortunately opened up the opportunity for perpetrators to exploit the uncertainty aspects. Although IPv6 has more than enough addresses, it carries on this practice, thus perpetuates the issues. The White House recently identified the BGP as the key component of Internet security concerns:

https://bidenwhitehouse.archives.gov/oncd/briefing-room/2024/09/03/fact-sheet-biden-harris-administration-releases-roadmap-to-enhance-internet-routing-security/

With the EzIP operations based on static address configurations and bounded L3 packet forwarding, much of the dynamic protocols, not only BGP, but also DHCP, DNS and AS are no longer relied upon. Thus, the Internet will become more secure against intrusions.

Authors' Addresses

Abraham Y. Chen
Avinta Communications, Inc.
142 N. Milpitas Blvd., #148, Milpitas, CA 95035-4401 US

Phone: +1(408)942-1485
Email: AYChen@Avinta.com

Abhay Karandikar
Director, India Institute of Technology Kanpur
Kanpur - 208 016, U.P., IN

Phone: (+91)512 256 7220
Email: Director@IITK.ac.in

Ramamurthy R. Ati
Avinta Communications, Inc.
142 N. Milpitas Blvd., #148, Milpitas, CA 95035-4401 US

Phone: +1(408)458-7109
Email: rama_ati@outlook.com

David R. Crowe
Wireless Telecom Consultant and Forensic Expert Witness
102 Point Drive NW, Calgary, Alberta, T3B 5B3, CA

Phone: +1(403)289-6609
Email: David.Crowe@CNP-wireless.com