ISSN: 2414-1895 DOI: 10.6919/ICJE.202109_7(9).0061

Internet Protocol Version 6 Migration

Jiayi Xu[1,*], Guozhen Miao[2], Mengfong Lio[3], Zehao Liu[4]

[1]Shenzhen Senior High School, Shenzhen, 518040, China;

[2]Maranatha High School, Pasadena, 91105, United States;

[3]Cleveland STEM High School, Seattle, 98118, United States;

[4]Jiangxi University of Technology International School, Nanchang, 330029, China.

*Corresponding author. Email: kellyjiayixu@gmail.com

Abstract

The internet is a very important development in the world today. There are many protocols that protect and govern the internet so that it is safe for people to use. One of these protocols is IPV4, which was developed in 1984. But as time goes on, we are having more and more problems with IPv4, so we developed another protocol, IPv6 which will hopefully take IPv4's place. We are going to view the necessary things in transitioning from IPv4 to IPv6.

Keywords

Internet; IPv4; IPv6.

1. Introduction

IPv6 is the newest internet Protocol, developed by internet Engineering Task Force in December 1995. The main mission of IPv6 is to replace and help IPv4 to solve its problem, which is lack of IP addresses. IPv6 uses a 128-bit IP address, compare to 32-bit for IPv4. Also, the IPv6 address format is longer than IPv4's because IPv6 can provide a larger amount of address sizes. Base on the big gap between them. so there needs to be a transition, and this process is slow because of many difficulties such as routing packets across incompatible networks. Despite the transition is slow, the use of IPv6 is more and more common, the world now has 20 to 22 percent IPv6 adoption.

2. Backgr0und

Transitioning from IPv4 to IPv6, several pivotal changes have been made. The reason why we need to transition to IPv6 is that IPv6 provides a way better service including having a larger address space, IPsec, extension header, and many other functions.

2.1 Larger Address space

As said in the introduction, IPv6 uses a 128-bit address space much bigger space than IPv4. This larger address space would mean that we will not have to worry about insufficient addresses in the future.

2.2 IPsec

IPsec known as internet Protocol security allows security to be at the IP level which is a feature of IPv6. This protocol mandates end systems such as routers to support a basic level of security. This would allow the use of non-secure applications.

ISSN: 2414-1895 DOI: 10.6919/ICJE.202109_7(9).0061

2.3 Extension Header

Extension header is an improved mechanism. It has an optional field that allows the extensions of the protocol. Differed from IPv4, most IPv6 extension headers will not be examined by the router until the packet arrives at the destination. This improvement makes IPv6 fragmentation different from IPv4 fragmentation.

The following chapters will expand upon specific problems in the transitioning process and some solutions that have been found.

3. Migration

Until 2013, IPv6 and IPv4 are basically on show same performance. The transition from IPv4 to IPv6 involves 2 key factors. The first factor is the availability and stability of IPv6. The second factor is the adoption by stakeholders.

3.1 Key factors

Availability and stability of IPv6: The early experience of using IPv6 was initially lagging behind IPv4. The main reason comes from the data plane. Until 2009, data plane performance is on par performance-wise. The control plane factors became the main contributors. IPv4 and IPv6 decision differ on routing, IPv6 will tunnel around routing that have not deployed IPv6 or not establish IPv6 peering sessions. Thus, speed became a problem. Until 2013, with the number of users of IPv6 increase, more routers adopt IPv6. It is now able to ensure that even with the difference of the control plane, the impact will be negligible.

3.1.1 Adoption by stakeholders

Stakeholders are ITDs, IsPs, ICPs, and users. ITDs build the technologies behind the internet. ITDs build the technologies behind the internet. ICPs take the charge of providing content on the internet. After IsPs purchase internet from ITDs, they provide connectivity to ICPs and users. At last, users will visit on the internet. After IsPs upgrade network to IPv6, adoption among major transit IsPs starts to increase significantly. By 2009, barely 500 or just 2 percentage of as were IPv6-capable. In the next two years from 2009 to 2011, the number increased from 500 to 1183, and the trend continued by late 2013. Meanwhile, ICPs increased accessibility of the IPv6. Until mid-2014, the accessibility grew up to 5 percent. After a relatively slow start, IPv6 is now supported by all major internet technologies.

3.2 Ecosystem Changes

The IPv6 ecosystem also changes as the adoption from ICP and IsPs increases. Ecosystem changes in mainly 6 ways.

3.2.1 The Demand for IPv6 Tech Changes

there were nearly zero demands for IPv6 in 1995 while it just came out. After IPv4 addresses run short, IPv6 is in substantial demand.

3.2.2 Unused IPv4 Address Commercial

About 30 percent of all public IPv4 addresses is still unused. Thus, mechanisms start to promote those unused addresses. Finally, these IPv4 addresses sales at prices ranging from 7 to 18 dollars in 2013 and 2014.

3.2.3 Infrastructure Upgrade Costs

Upgrading infrastructure for IsPs to supporting IPv6 is a huge number of tasks which include upgrading of equipment and operation. Upgrading cost is tightly linked with the size and complexity of infrastructure.

All in all, upgrading costs will increase with the scale of the infrastructure increases, and it will also decrease with the technology matures. The same situation is for ICPs. Labor and hardware, or software equipment, costs are the main costs.

ISSN: 2414-1895 DOI: 10.6919/ICJE.202109_7(9).0061

3.2.4 Translation Costs

To allow connectivity to the public, IPv6 and private IPv4 addresses need to be translated. Costs by translation are proportional to the volume of traffic that needs to be translated.

3.2.5 The Number of Users has been steadily Increasing

The large number of IPv6 users will urge ICPs to become more IPv6- accessible and make IsPs more focus on IPv6.

3.2.6 Technology Maturity

With the improvement of the stability and performance, IPv6 initially to be on par with IPv4 in some cases even better. Greater technology maturity is not the only factor behind the par performance-wise between IPv6 and IPv4. End-to-end connectivity is affected by both end-systems and the network. For end-systems, IPv6 support in end-systems is decided by ITDs. IPv6 availability was initially not stable across 0ss. However, it is not a concern nowadays anymore. Moreover, ITDs' ability to upgrades packet forwarding performance in IPv6 decided the routers' ability to forward IPv6 packets. The path connecting to the destination chosen by IPv6 is not only affected by ITDs but also IsPs.[1]

4. Tunnels

Tunneling is an important step in transitioning from IPv4 to IPv6. Its use is to bridge compatible networking nodes across networks that are not compatible. It encapsulates a payload at the entrance and then transfers it through the tunnel to the exit, where the payload is decapsulated. In the transition from IPv4 to IPv6, the most notable use of tunneling is to bridge incompatible IP segments, like transferring an IPv6 payload over an IPv4 network or vice versa. There are three tunneling mechanisms proposed by the Internet Engineering Task Force and two main solutions, configured IP-in-IP Tunneling and 6to4 Automatic Tunneling.

4.1 Mechanisms

The mechanisms behind tunneling proposed by the IETF are 6over4, IsATAP, and DsTM.

4.1.1 6over4

6over4 (IETF RFC 2529) allows the transfer of IPv6 payloads across an IPv4 network. This is accomplished by putting IPv4 addresses in the IPv6 addresses' last 64 bits, the link layer identifier part. It defines Neighbor Discovery over IPv4 by using organization-local multicast. This means that the sender determines the IPv6 address over the IPv4 network using Neighbor Discovery. This address contains the IPv4 address of the destination tunnel endpoint.

4.1.2 IsATAP

The Intra-site Automatic Tunnel Addressing Protocol (IsATAP) allows two disconnected IPv6 routers to be connected with tunneling. In this protocol, the tunneling is automated with IPv6-IPv4 compatible addresses.

4.1.3 DsTM

The Dual-stack Transition Mechanism (DsTM) allows IPv4 packets to be tunneled across an IPv6 network by allocating a temporary IPv4 address to the dual-stacked end systems on the IPv6 network.

4.2 Solutions

There are two main solutions that the IETF had proposed for interconnection across incompatible networks, configured IP-in-IP tunneling and 6to4 automatic tunneling.

4.2.1 Configured IP-in-IP Tunneling

In this type, the nodes within the network are configured for tunneling. A tunnel broker, which alleviates the management effort required, is used to manage tunneling parameters. The tunnel broker provides services that return the scripts and parameters for the tunnel configuration. Even though this type of tunneling requires more management because of the initial deployment and the fact that both tunnel endpoints need to be configured, this provides better network Qos.

ISSN: 2414-1895 DOI: 10.6919/ICJE.202109_7(9).0061

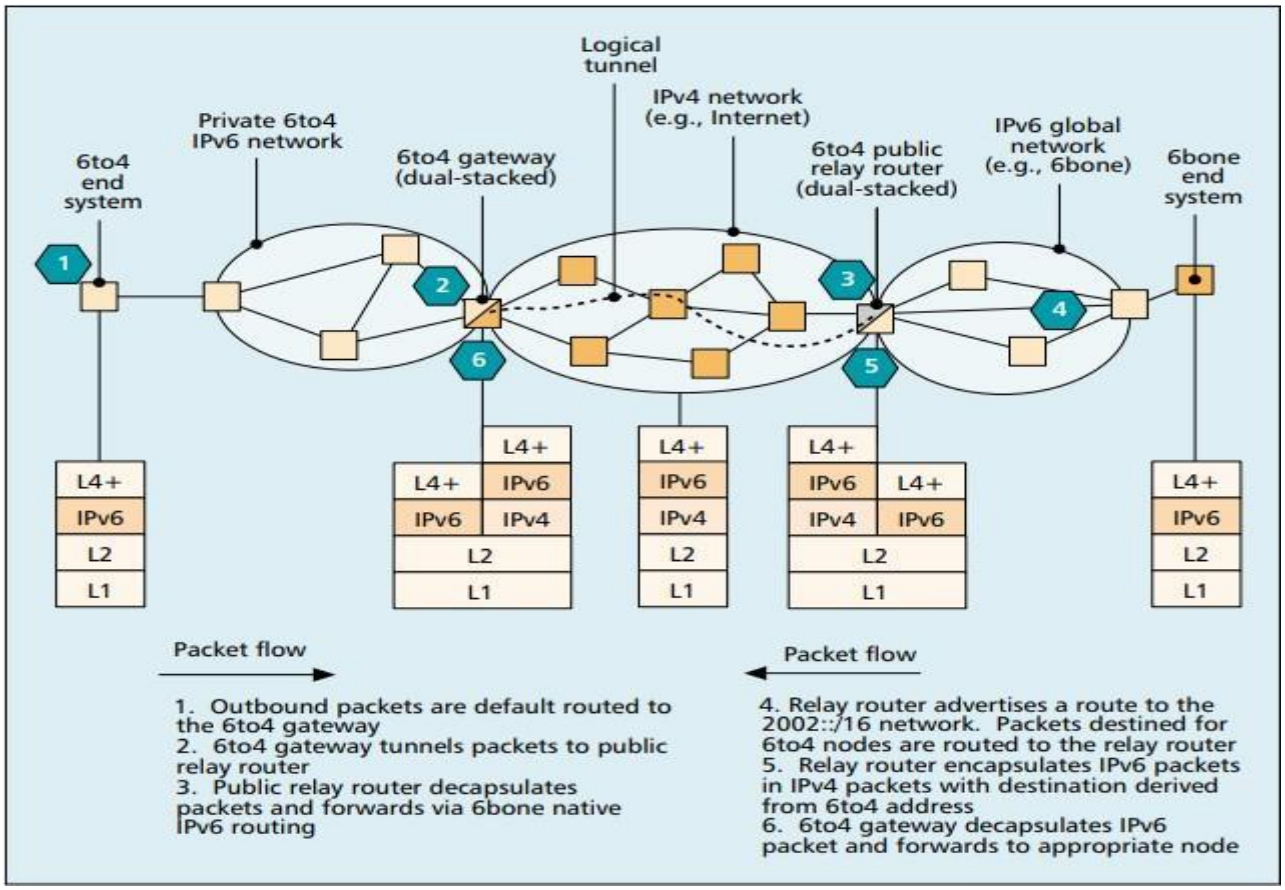

Fig. 1 6to4 Automatic Tunneling

4.2.2 6to4 Automatic Tunneling

This type of tunneling does not require the management that is needed for tunnel configuration. The automation is achieved by techniques such as 6to4. 6to4 mechanism transfers IPv6 payload across an IPv4 network among isolated 6to4 networks. Each of the 6to4 networks has a prefix containing their IPv4 address of its 6to4 gateway. This allows obtaining tunnel endpoint addresses to be automatic and simple. Figure 1 shows a 6to4 tunneling connecting a 6to4 network to the 6Bone, an IPv6 network, via the IPv4 Internet. Since this type of tunneling requires little management, this can be unreliable as only one tunnel endpoint is configured. This would also block the use of multicast and anycast.

Tunneling is an important solution to some of the problems during the process of transitioning from IPv4 to IPv6. There are solutions proposed by the IETF such as configured tunnels and 6to4 automatic tunnels which use mechanisms such as 6over4, IsATAP, and DsTM. Even though there are advantages and disadvantages to both solutions, we are coming up with solutions faster and we are pushing towards the global use of IPv6. [2]

5. Fragmentati0n

To entirely change IPv4 to IPv6, one of the major points needed to consider is the IP packet fragmentation.

Unlike fixed-size packets in time-switched network for telephony, packets in packet-switched network can have different sizes. While smaller packets can be dispatched faster as well as reducing head-of-line blocking and jitter, larger packets have a higher carriage capacity and higher-speed network systems. Consequently, small packets are likely to be used in delay-sensitive and real-time applications. The reliable bulk data transfer, however, may prefer to use larger packets because they have a larger carriage efficiency. However, because of the Maximum Transmission Unit (MTU), the size of each packet should be considered. In IPv4, if the application sends a packet too large, it

ISSN: 2414-1895 DOI: 10.6919/ICJE.202109_7(9).0061

requires the packet to be fragmented. The idea is to break a large packet into a set of smaller “fragments" with the same IP header fields. If the router receives a packet larger than the next hop's MTU, it will either drop it or further fragment it, which depends on the f1ag setting in the packet's header. If the f1ag is Don't Fragment (DF), the router will drop the packet and send an Internet Control Message Protocol (ICMP) message, signaling to the packet source that fragmentation is needed. 0therwise, it will further fragment the packet. As soon as they reach the destination host, they will be reassembled and passed to the higher protocol layer.

However, there are a few changes in IPv6 fragmentation. In IPv6, fragmentation is not allowed in the transmission so that the routers do not fragment the packets. If the packet is too large, it will be dropped.

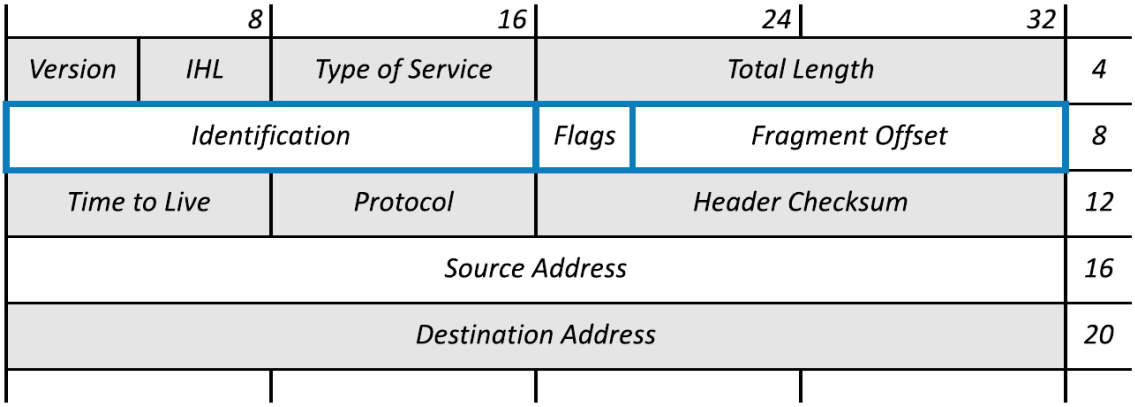

Fig. 2 IPv4 Fragmentation

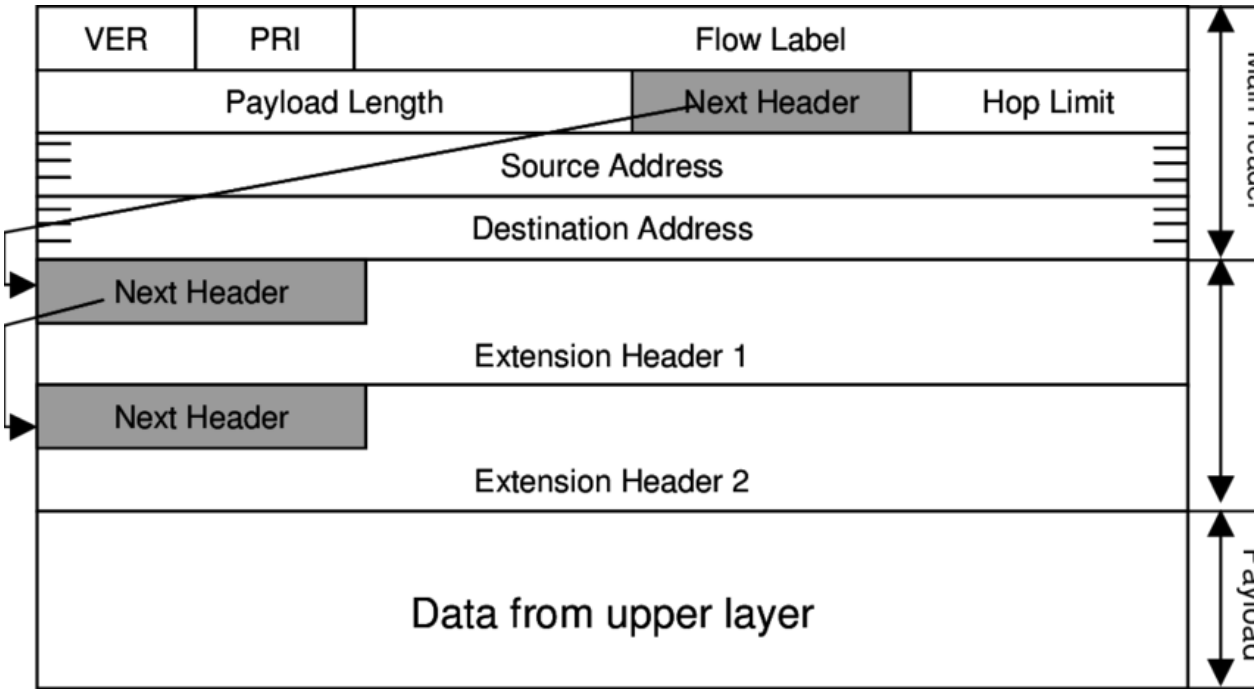

Fig. 3 IPv6 Datagram

Packet Too Big (PTB) will be sent to the source, indicating further fragmentation is needed. The host can find out the maximum packet size with the help of the Path MTU Discovery protocol (PMTUD). Moreover, one of the pivotal structures in IPv6 packet is the Extension Header, which carries optional

ISSN: 2414-1895 DOI: 10.6919/ICJE.202109_7(9).0061

internet layer information such as routing, fragment, and authentication. If the upper-layer protocols are unable to limit the payload size, the host might use the information carried on the extension header to help with the fragmentation of the IPv6 packets.

The fragmentation seems to enable IP packets to traverse any media since adaptations can be made easily. However, it still earns a poor reputation and is even considered harmful because of its drawbacks such as performance inefficiency and security vulnerability.

For Transmission Controlled Protocol (TCP), the packets with Extension Headers have a high dropping probability. According to the experiment in Huston's paper [3], the overall failure rate is as high as 21%, meaning that almost one-fifth of the users may fail to receive fragmented large responses. How to reduce the failure rate of acknowledging fragmented TCP packets becomes a serious problem in the IPv6 network.

Table 1. Results of IPV6 Fragmentation test

	count	Percentage
sent Fragmented TCP Packets	1,675,898	
Acknowledged Fragmented TCP Packets	1,324,834	79.03%
Failed to Acknowledge	351,514	20.97%

Compared to fragmentation in TCP, fragmentation in User Datagram Protocol (UDP) brings people more serious problems. The Domain Name System (DNS) is a major user of UDP. 0ne of the most serious problems is the security problem of the firewall, which helps to monitor and filter the incoming and outcoming traffic. The headers of IP packets can provide the basic information for the firewalls to inspect and determine whether to admit or deny them. In IPv6 packets, the number of extension headers for each packet is not limited, which largely creates more work for firewalls to identify and deal with numerous extension headers. This might also create some opportunities for attackers to deliberately add many extension headers to the packets, which leads to a waste of resources. Moreover, the attackers can send some duplicated fragments in an attempt to interfere with the process of reassembling so that they can destroy the filtering function of the firewalls.

In conclusion, today's network cannot live without the design of fragmentation. However, the IP fragmentation facilities in IPv6 is still not mature enough to meet the needs of the internet. To have a brighter future of IPv6, more improvements are needed.

6. Target generati0n

Scanning here mostly use in security assessments and also can help to perform hackers' attacks. But IPv6 address space is too big, so it is impossible to exhaustively scan. Although this will be a problem for IPv6 scanning, this scanning still needs to happen. Because there aren't any more spaces for IPv4 addresses.

Some more background about IPv6 addresses is represented in a format of using eight groups of numbers, and each group is four hexadecimal digits. IPv4 can provide around 4.29 billion space, and currently, there are 4.021 billion people are using it. So IPv6 became more necessary to exist. Because IPv6 can provide a huger number of addresses per person than IPv4, it came out a big task for the scanning process.

While talking about prior work, there are some considerations for IPv6 scanning. One of the important points is that the target generation has to be reliable and can be scan largely.

The target generation algorithm, 6Gen, has to be introduced. 6Gen can put all the similar seeds together with a high speed, and use those addresses within the region as a target. Seed is a number or other value that is generated by software using one or more values. Seed means a random number generated by the computer, which is useful to machine learning and data collection. But before putting

ISSN: 2414-1895 DOI: 10.6919/ICJE.202109_7(9).0061

all the similar seeds together, 6Gen had to firstly identify those seeds and decide whether it is similar or not. Although it is possible to gather different densities, the budget for this process will be too high. Budget in here means the amount spent on the scanning process. To be able to say which address is similar to which, 6Gen has to define a similar metric. The metric counts the number of nibbles (a four-bit aggregation). Positions are different between two addresses to calculate the distance between two regions of IP space [4]. The main process is using range to put all the seeds together. In the process, 6Gen first identifies the closest seed to cluster based on the Hamming distance. When each of the potential clusters grows, the cluster range would expand, which seeds to set growth. The paper notes that the algorithm can result in overlapped clusters because every non-cluster seed for potential growth, and grow clusters independently [4]. The algorithm can also result in the overlapped cluster.

The next part talks about the 6Gen's Cluster, which is shown in figure 5. Although 6Gen has been introduced, more future works have to do. IPv6 De-aliasing, scanner integration, and deeper exploration are needed for Target Generation Algorithms. In IPv6 De-aliasing, further exploration is needed to develop scalable and reliable alias resolution, to better understand the topology of the IPv6 Internet, and to more accurately characterize IPv6 scanner performance [4].

This paper lists out the basic challenges for 6Gen and Target Generation IPv6 scan, and also what needs to be done in the future. 6Gen has highlighted important areas for IPv6 target generation. But target generation must become more high-tech to become more economically worthy and effective.

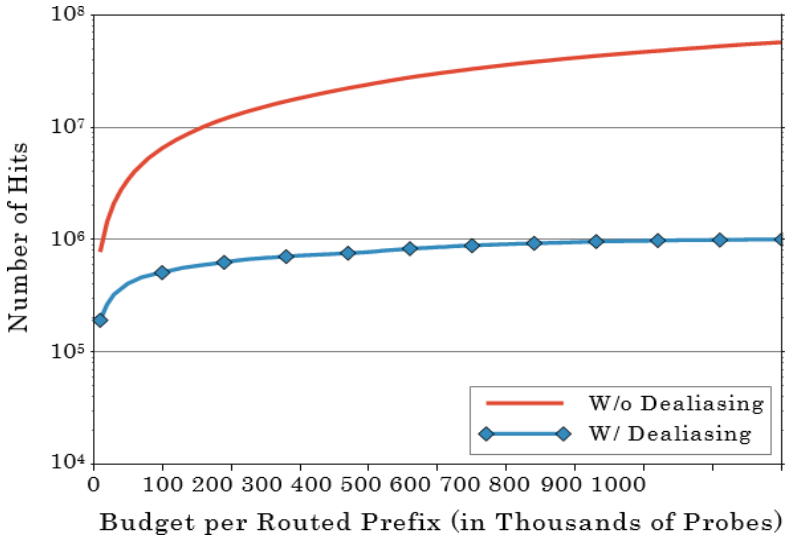

Fig. 4 Target Generation

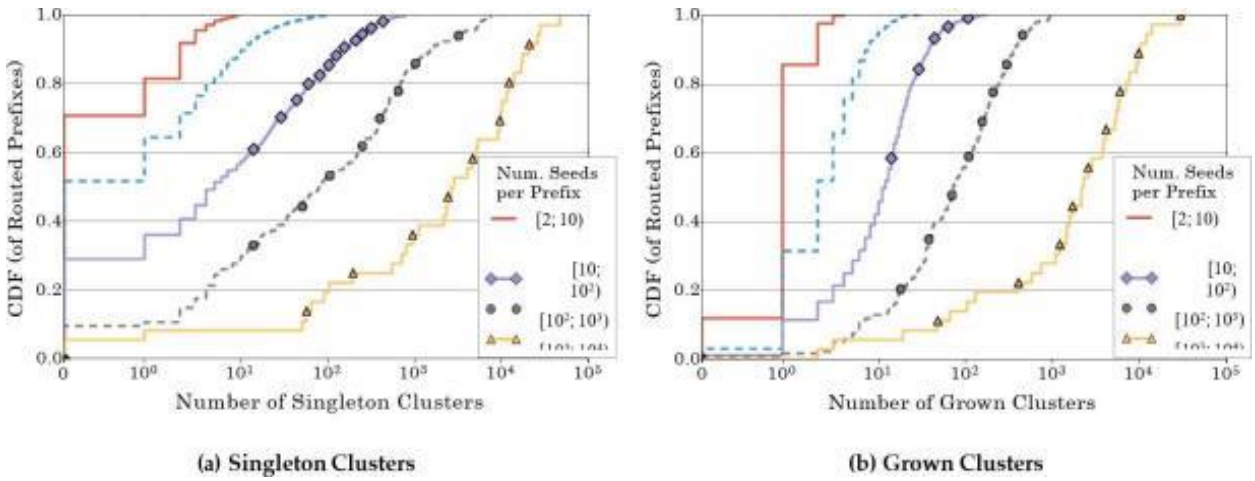

Fig. 5 Target Generation

ISSN: 2414-1895 DOI: 10.6919/ICJE.202109_7(9).0061

Algorithm 1 6Gen pseudocode, simplified to illustrate conceptual steps, and without optimizations (see §5.5).

```
clusterList = []

function InitClusters(seedList)
    for seed in seedList do
        cluster = new Cluster()
        cluster.addSeedUpdateRange(seed)
        clusterList.add(cluster)

function FindCandidateSeeds(cluster, seedList) ▷ Computes the minimum Hamming distance between cluster.range and all seeds in seedList not already in cluster, and returns the list of seeds that are this minimum distance away.

function GrowCluster(seedList)  ▷ Consider growing all clusters by candidate seeds, and select the growth resulting in the highest seed density and smallest cluster range size.
    maxDensity, maxIndex, maxRangeSize = 0, 0, Infinity
    maxCluster = None
    for index in [0, ..., clusterList.length() − 1] do
        cluster = clusterList[index]
        candidateSeeds = FindCandidateSeeds(cluster, seedList)
        for seed in candidateSeeds do
            tmpCluster = cluster.copy()
            tmpCluster.addSeedUpdateRange(seed)
            for otherSeed in candidateSeeds do
                if otherSeed in tmpCluster.range then
                    tmpCluster.addSeedUpdateRange(otherSeed)
    ▷ Does not further change the range.
            newDensity = tmpCluster.seedSet.size() / tmpCluster.range.size()
            if (newDensity > maxDensity) or (newDensity == maxDensity and tmpCluster.range.size() < maxRangeSize) then
                maxDensity, maxIndex = newDensity, index
                maxRangeSize = tmpCluster.range.size()
                maxCluster = tmpCluster
    return (maxIndex, maxCluster)

function 6Gen(seedList, budgetLimit)  ▷ Grow clusters until the sum of cluster range sizes exceeds the budget. For simplicity, we elide here details about handling cluster overlap and final cluster growth sampling to use up the budget exactly.
    InitCluster(seedList)
    budgetUsed = 0
    while True do
        grownIndex, grownCluster = GrowCluster(seedList)
        oldRangeSize = clusterList[grownIndex].range.size()
        newRangeSize = grownCluster.range.size()
        budgetCost = newRangeSize − oldRangeSize
        budgetUsed = budgetUsed + budgetCost
        if (budgetUsed ≤ budgetLimit) and (seedList.size() > grownCluster.seedSet.size()) then
            clusterList[grownIndex] = grownCluster
        else
            return clusterList
```

Fig. 6 Target Generation

ISSN: 2414-1895 DOI: 10.6919/ICJE.202109_7(9).0061

7. Conclusion

Nowadays, the whole society is currently transitioning from the old version IPv4 to this new version. The main function of IPv6 is to replace and help IPv4 to solve its problem. Even though the transitioning is happening, this process is slow because of many difficulties such as routing packets across incompatible networks. But scientists are also coming up with different solutions such as tunneling, targeting, and fragmentation which allows having more IPv6 connectivity. It is reasonable to believe the future of IPv6 is brighter and brighter.

Acknowledgments

We would like to thank professor Bill Nace and teachingS assistant Zhenyi Ye for their instructions.

References

[1] M. Nikkhah and R. Guerin, “Migrating the Internet to IPv6: An Exploration of the When and Why,” IEEE/ ACM Transactions on Networking, vol. 24, no. 4, pp. 2291–2304, 2016.

[2] D. Waddington and F. Chang, “Realizing the transition to IPv6,” IEEE Communications Magazine, vol. 40, no. 6, pp. 138–148, 2002.

[3] G. Huston, “IPv6 and Packet Fragmentation,” Internet Protocol Journal, Apr. 2018.

[4] A. Murdock, F. Li, P. Bramsen, Z. Durumeric, and V. Paxson, “Target generation for internet-wide IPv6 scanning,” Proceedings of the 2017 Internet Measurement Conference, 2017.