Student ID: 19614652

Student Name: Jia Son Pow

Report on IPv4 and IPv6

Table of Contents

1. **Introduction to IPv4 and IPv6** 2
2. **Challenges in IPv4** 2
3. **IPv6 Solutions** 3
    a. **Capacity** 3
    b. **QoS** 5
    c. **Security** 5
    d. **Efficient Routing** 6
    e. **Efficient Dataflow** 8
    f. **Maintaining Large Routing Tables at Internet Backbone Routers** 10
4. **Challenges in Migrating from IPv4 to IPv6** 10
5. **Conclusion** 11
6. **Bibliography** 12

1. Introduction to IPv4 and IPv6

The Internet Protocol, which forms the basis of all communications on the Internet, is the official framework used for information exchange. The IP utilizes a specialized system for addressing to specify source and destination of communication. IPv4 is the abbreviation of Internet Protocol version Four and it is one of four core protocols maintained in the standards-based networking methods on the Internet. IPv4 was released in 1978 and remains in use today for most internet traffic as it was the first version of Internet Protocol to be widely deployed. IPv6, short for Internet Protocol version Six, is the latest revision of the Internet Protocol which is developed by the Internet Engineering Task Force in 1995 as a countermeasure to the long-foreseen depletion of the pool of unoccupied IPv4 addresses.

2. Challenges in IPv4

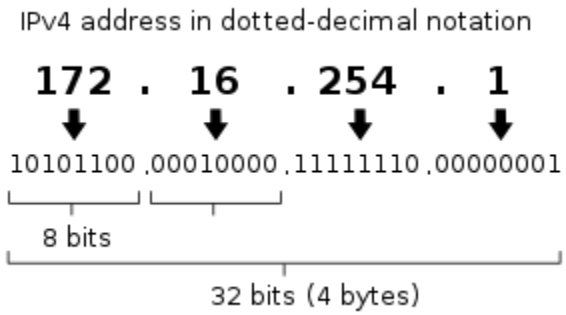

Figure-1

The IPv4 uses a 32-bit identifier normally exhibited in quad-dotted notations, each in the range of 0 to 255, which can generate approximately 4.3 billion addresses (2^{32} unique combinations) as illustrated in Figure-1. This was stipulated to be inexhaustible at the time as this version of Internet Protocol was developed as part of a conceptual internetworking test project led by the Defense Advanced Research Projects Agency in the USA. However, by the year 1992, the IPv4 addressing system was posed with many problems as the commercialization of Internet has driven rapid growth in number of addresses being occupied in the IPv4 address space. Inherently, due to its primitive nature as a test project, the IPv4 has only the most basic quality of service capabilities and lacks encryption features. (Zhang, 2007) Due to the shortage of addresses, Network Address Translation (NAT) was introduced as a

countermeasure. A NAT router acts as an intermediary exchange between the global Internet and private IPs, where it will have a public address for its interface facing the Internet and a private address facing the private IPs. When a private IP wants to send out a packet to the Internet, the packet goes through the NAT router where the router will translate the private source IP address on the packet's header into a public IP address before the packet is sent to the destination address. The router will also keep a record on its internal mapping table should a situation arises where the public IP on the outside wants to send a response packet back into private IP, the router will find the corresponding entry and replace the public destination address on the packet with the real destination address so that it will be delivered to a private IP inside the network. This can be a static one-on-one mapping in the case of static NAT, or a dynamic mapping with a pool of public addresses.

Dynamic NAT has a limitation where the number of hosts that can use the Internet cannot be larger than the number of external addresses available in the NAT pool. This limitation can be overcome by NAT overloading where one-to-many address translations are provided by assigning a unique TCP/UDP port to each packet transferring session. This method was created as a short-term solution while a new IP is waiting to be developed as a long-term solution but it was quickly adopted by large enterprises as the instant gain in data transferring power can easily be seen. However, its drawbacks were slow to show and under awareness when it was already too late. NAT overloading breaks the end-to-end principle, a design method that removes critical components from intermediary nodes to increase routing options, improve data delivery rates and make sure applications only fail if the end point fails. (Grundermann, n.d.) Large scale NAT routing are also able to break applications such as VoIP applications, video streams, FTP downloads and many others. (Donley, 2011)

3. IPv6 Solutions

a. Capacity

The IP address space is managed globally by the Internet Assigned Numbers Authority, with five regional Internet registries responsible for the allocation of address space within specified geographical areas. Local Internet Registries (LIRs), typically, internet service providers (ISPs), are

allocated blocks of addresses, and they, in turn, assign that space to their customers for exclusive use in their networks.

In recent years, IPv4 addresses have been assigned at a rate never seen before as many countries in the world have had rapid economic growth and the demand for addresses have followed suit as a result. The Internet Assigned Numbers Authority's primary address pool was exhausted on February 3, 2011, when the last 5 blocks were allocated to the 5 RIRs. As of mid-2014, AFRICNIC, the RIR responsible for the region of Africa, remains the only registry to supply IPv4 addresses to network providers in its service region. (Levin, 2014) The issue of IPv4 address exhaustion is no longer just a theoretical trajectory but a reality that demands urgent attention from governments, network operators and end users.

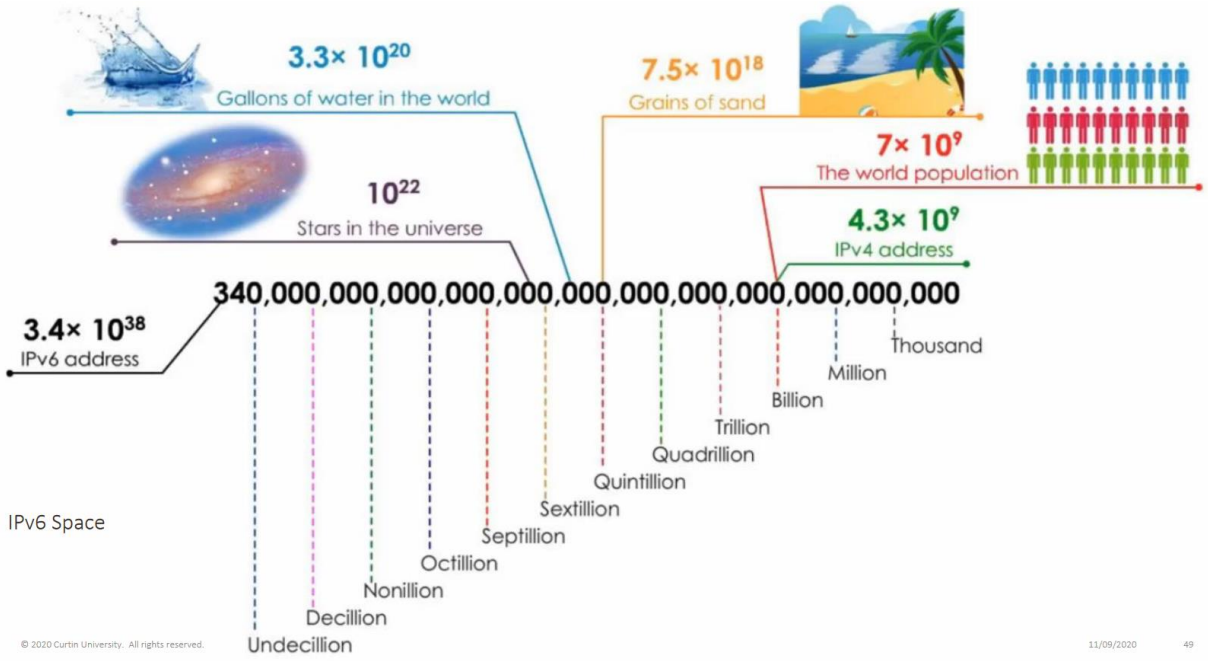

Figure-2

On the other hand, the IPv6 protocol, which utilizes a 128-bit identifier, consists of 8 numbered strings, each of them containing 4 characters, separated by a colon. This gives us an unfathomable number of supported devices, 340 undecillions to be exact. Figure-2 above serves a guidance to the scale of both IPv4 and IPv6 address space with comparison to other forms of

space. From that, we can be sure that we will not be running out of address spaces anytime soon once IPv6 is fully adopted.

b. QoS

Quality of Service is the measurement of a service's performance, in particular the performance seen by users of the service network. It is of utmost importance because without it, the end users may encounter many issues like packet loss, latency and speed jitters.

In IPv4, flow classification is based on the fields: source and destination IP address type of transport layer protocol and ports. However, due to fragmentation or encryption of packets on the network, some of these fields may not be available. (Parra et al.,2011)

In contrast, these problems have been overcome in the IPv6 flow classification where a flow label field is used by the source nodes and intermediate routers to identify and distinguish between different classes or priorities of IPv6 packets. Usage of the flow label field helps reduce processing load of network routers which in turn reduces the end-to-end delays of packets. The reservation of resources through the flow label also means the problems encountered by a high frequency of route changes are negligible.

c. Security

Network security is one of the most important aspects to consider when building a network of hosts. A stable and efficient network security system ensures that the data inside the client servers will be well protected. Network security promotes reliability of your network by preventing lagging and downtimes through continuous monitoring of any suspicious transaction that can sabotage the system.

The declining number of IP addresses is a major concern for IPv4 as the aforementioned 4.3 billion addresses have long been outnumbered by the number of people in the world right now. NAT technology provides security to the network as it hides the internal users from the outer public

network. However, this also means that there are no means provided to limit access to information hosted on the network as the IPv4 has never been designed for security.

However, on IPv6, Unique Local Addressing is used to protect the users' IP addresses where they may be used freely within the scope of a private network but not in the global IPv6 Internet. IPv6 also contains a mandatory security feature, IPSec, in its standards. IPSec is a series of IETF security protocols for security, authentication, and data integrity, and it is fully integrated into IPv6. IPv6 provides two security headers. They are the Authentication Header (AH) and Encapsulating Security Payload (ESP). AH provides data-origin authentication and protection against replay attacks, while ESP delivers connectionless integrity, limited traffic flow confidentiality, privacy and confidentiality through encryption of the payload.

d. Efficient Routing

When the Internet was first created, it was quickly realized by the developers that it would be shared by many organizations of different sizes and there was a need to have a system in place whereby the IP address space would be divided into classes, where each of them would contain a portion of the total number of addresses and had been dedicated to specific uses. This is known as the "classful" addressing scheme. This method was developed at a time for a network that was limited in size and not expected to have grown as much as it is in the current day. This led to three major problems: lack of internal address flexibility, inefficient use of address space and proliferation of router table entries.

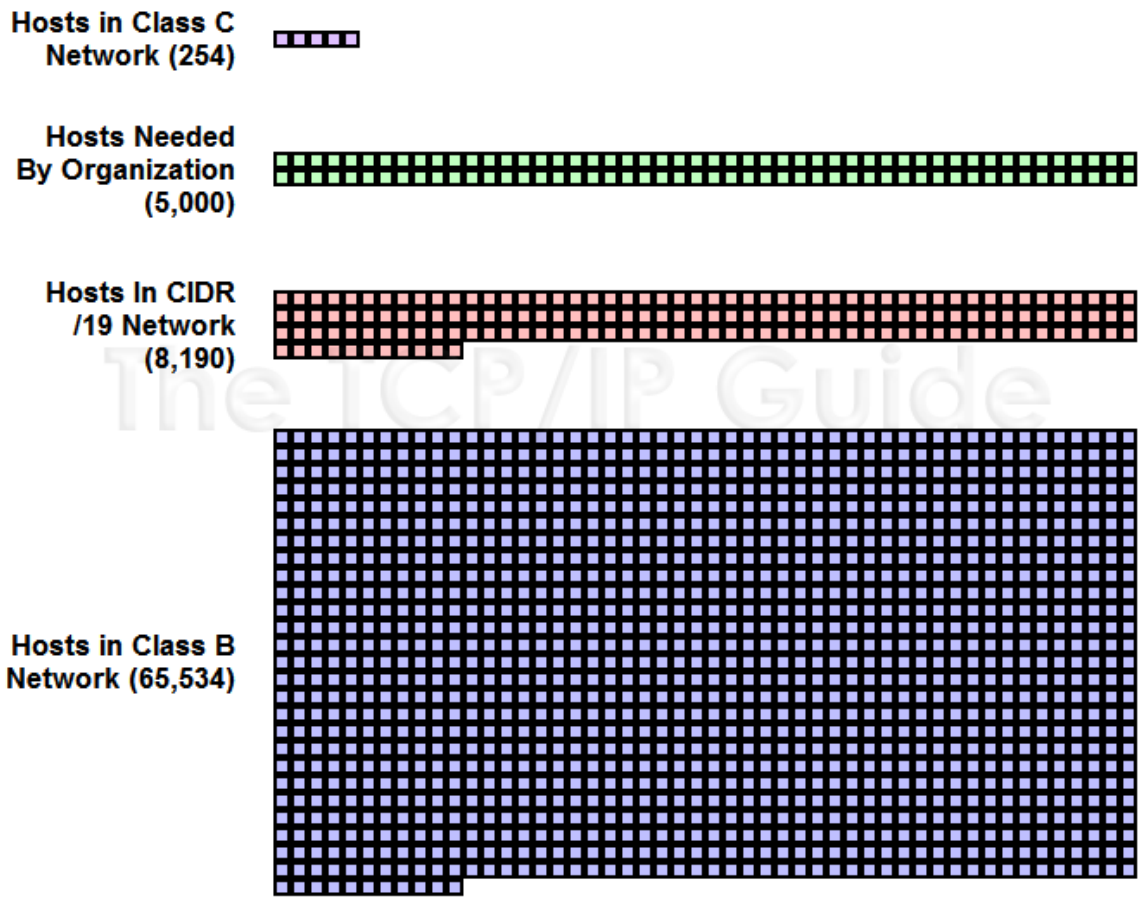

Figure-3

As can be seen above in Figure 3, each square represents 50 available addresses. Since a Class C address has only 254 addresses, and a Class B contains 65,534 addresses, an organization with 5,000 hosts is "caught in the middle". It can only choose to either waste 90% of a Class B address or use 20 different Class C networks. This is highly prevalent in most of IPv4 networks today.

To counteract this problem, the IPv6 utilizes Classless Inter-Domain Routing (CIDR). The idea behind this routing method is that instead of breaking a particular network into subnets, more networks are aggregated into larger "supernets". As illustrated above, in the case of a 5000-host organization, a /19 network with 8,190 hosts can be assigned. This greatly reduces the address space waste by about 95%.

e. Efficient Dataflow

IP routing is a process in which packets will be forwarded from one node to another. The choice of IP protocol can affect the routing performance. A datagram must be small enough to fit within the lower-layer frame at each step on the way for a datagram to be successfully carried along a route. Maximum transmission unit describes the size limit for any given network. If a datagram is too large for a network's MTU, it will be broken down into smaller packets before being sent out.

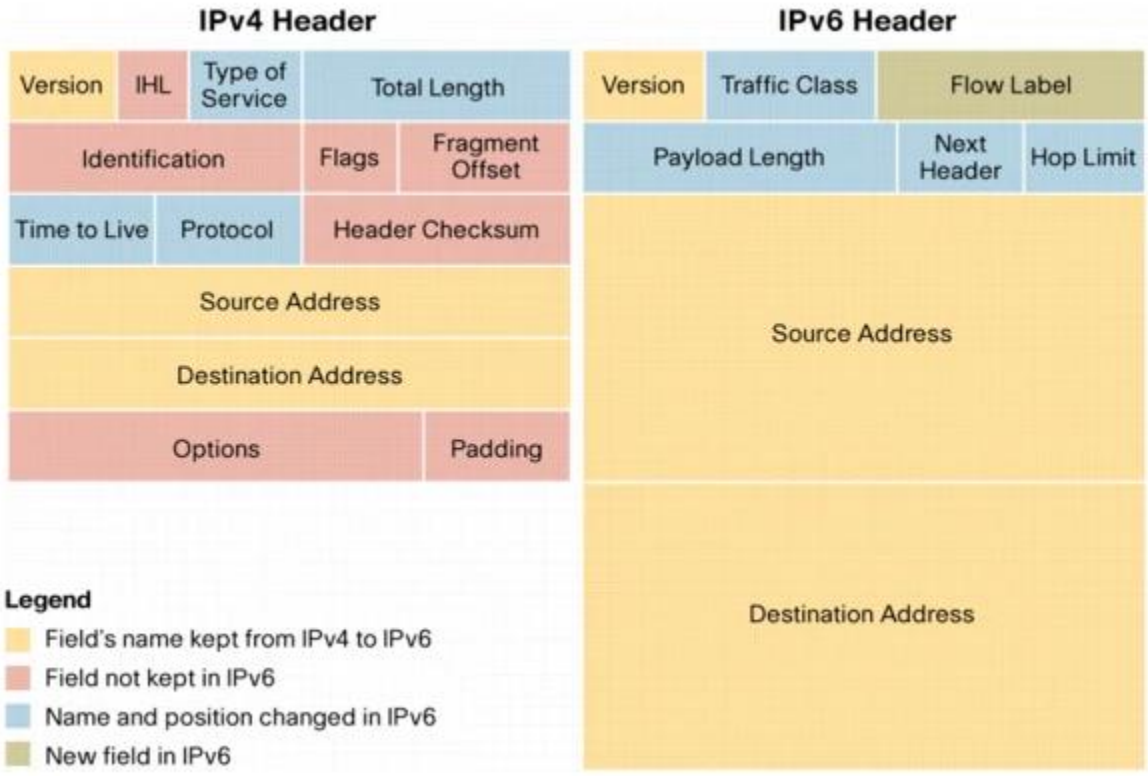

Figure-4

In IPv4, the minimum MTU that routers and physical links were required to handle was 576 bytes. Datagrams may be fragmented by either the source device, or by routers during delivery. This led many problems as this form of fragmentation posed vulnerabilities to hosts as malicious attackers could send a stream of fragments with similar identifier values to deceive the receiving host and overrun the network. Fragmentation can also cause excessive retransmissions when fragments encounter packet loss and reliable protocols such as TCP must retransmit all the fragments to recover from the loss of a single fragment. (Kozierok, 2005)

On the other hand, in IPv6, all links must handle a datagram size of at least 1280 bytes. As can be seen above in Figure-4, this more-than-doubling in size improves efficiency by increasing the ratio of maximum payload to header length and reduces the frequency with which fragmentation is required. In IPv6, only the source node can fragment, the routers do not. The source must therefore fragment to the size of the smallest MTU on the route before transmission. This ensures that there will be little to no packet loss as the packets will not encounter any form of en-route fragmentation by routers for the entirety of the chosen link route (Huston, 2016). Figure-5 below shows an example of how a 370-byte IPv6 datagram is broken down into three fragments. The parts marked in purple are unfragmentable as these headers are required at each step of the way for the packet to reach its destination while hopping over different nodes. Parts marked in green are fragmentable parts which include Authentication Header and Destination Options Header alongside the carried data.

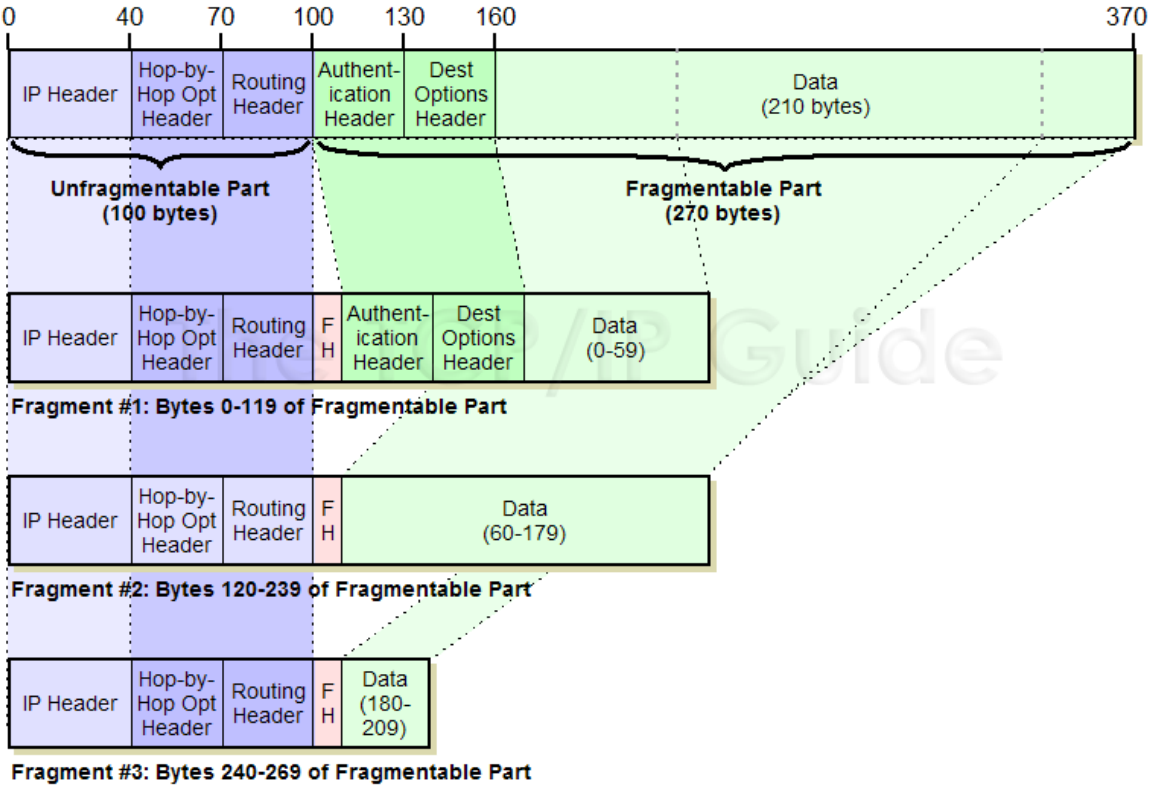

Figure-5

f. Maintaining Large Routing Tables at Internet Backbone Routers

In networking, a routing table is used to list routes to network destinations and the metrics linked to those routes. The allocation of Class C (blocks of 256 contiguous IPv4 addresses) networks instead of Class B networks has led to an alarming expansion of the routing tables in the Internet backbone routers.

To address this problem, a new addressing method called subnet addressing was developed for the IPv4. This essentially allows organizations to have their own private network whilst being in a public Internet network. This allows hosts to be grouped into subnets which mirrors how they are structured in the organizational network. It also provides great flexibility as each organization can customize their own subnet structure and change as required. This also provides more privacy to the organizations as the internal subnet structure is not visible to the public network. Most importantly, since the subnet structure only exists within the organization, there will be no routing table entry proliferations since an organization will no longer need to have a routing table entry for every single one of its devices. (Dordal, n.d.)

However, although subnetting decreases the total number of IP addresses in the network, the organizations may need buying additional hardware to sustain the additional routing that needs to be in place for these subnets and it may cost a lot of money. Also, it does not increase the network efficiency since the organizations are still assigning address block regarding to classes.

With IPv6, however, this will no longer be a concern as the IPv6 has an almost endless amount of address spaces to provide for networking purposes enough for many years to come.

4. Challenges in Migrating from IPv4 to IPv6

In recent years, the IPv4 has been significantly updated to overcome some of its problems that may encourage large organizations to not migrate from IPv4 to IPv6. In terms of network security, the difference between IPv4 and IPv6 has been very little. The same IPSec in IPv6 is now made available

for IPv4 so it is in the hands of network providers and end users alike to embrace and use it. As for IP addressing, since the main benefit of "classful" addressing was its simplicity, it is no surprise at all that the main drawback of CIDR is its higher level of usage complexity. As it stands, it is no longer possible to determine by looking at the first octet to determine how many bits of an IP address represent the network ID and how many the host ID. Also, more care needs to be taken than usual when setting up routers to make sure that routing is accomplished correctly. With all that being said, there are a few solutions available that allows for better transition from the IPv4 to IPv6.

Given that IPv4 addresses will not disappear from the Internet any time soon, running a dual stack network with IPv4 and IPv6 deployed side-by-side is a measure that can be taken to counteract IP address scarcity without forgoing the legacy system in place.

Another alternative is a NAT64 gateway that facilitates the communication between IPv6 and IPv4 hosts and acts as a translator where traffic from the IPv6 network is routed via the gateway which performs all the necessary translations for transferring packets between the two networks. (Sunny's Classroom, 2019)

5. Conclusion

In conclusion, it can be seen that while there has been advancements in solving the problems found in IPv4, the truth is that IPv6 will soon become the only option to connect new devices and hosts to the Internet as the IPv4 address space will eventually be depleted completely. In addition, IPv6 simplifies and speeds up data transfer due to more efficient packet processing. As a result, the valuable working time of the router is released to perform its immediate tasks. Finally, IPv4 was not originally thought of as a secure protocol while IPv6 was designed from the very beginning in terms of protection. All these factors signify that the move to IPv6 will be essential for a sustainable global network.

6. Bibliography

Zhang, L 2007, *A Retrospective View of NAT*, viewed 15 Oct 2020, <https://www.ietfjournal.org/a-retrospective-view-of-nat/>

Grundermann, C (n.d.), *NAT444 (CGN/LSN) and What it Breaks*, viewed 15 Oct 2020 <https://chrisgrundemann.com/index.php/2011/nat444-cgn-lsn-breaks/#NAT>

Donley, C.D. 2011, *Assessing the Impact of NAT444 on Network Applications*, viewed 15 Oct 2020 <https://tools.ietf.org/id/draft-donley-nat444-impacts-00.html>

O. J. S. Parra, A. P. Rios and G. Lopez Rubio, "Quality of Service over IPV6 and IPV4," 2011 7th International Conference on Wireless Communications, Networking and Mobile Computing, Wuhan, 2011, pp. 1-4, doi: 10.1109/wicom.2011.6040165.

Levin, 2014, *IPv4 to IPv6: Challenges, solutions, and lessons*, viewed 16 Oct 2020 <https://www.sciencedirect.com/science/article/pii/S0308596114001128?via%3Dihub>

Dordal, P (n.d.), *An Introduction to Computer Networks*, viewed 16 Oct 2020 <http://intronetworks.cs.luc.edu/current/html/bigrouting.html>

Huston, G 2016, *Evaluating IPv4 and IPv6 packet fragmentation*, viewed 16 Oct 2020 <https://blog.apnic.net/2016/01/28/evaluating-ipv4-and-ipv6-packet-frangmentation/>

Sunny's Classroom (2019), *IPv4 to IPv6 transition - Translation with NAT64*, Available at: https://www.youtube.com/watch?v=EhCzKyojkNs (Accessed: 16 Oct 2020)

Kozierok, C 2005, *IP Variable Length Subnet Masking (VLSM),* viewed 17 Oct 2020, <http://www.tcpipguide.com/free/t_IPVariableLengthSubnetMaskingVLSM.htm>

Figure 1 - https://en.wikipedia.org/wiki/IP_address

Figure 2 - Computer Communications (CNCO2000) Lecture 5 slide no.49

Figure 3 - http://www.tcpipguide.com/free/t_ProblemsWithClassfulIPAddressing-2.htm

Figure 4 - https://www.cisco.com/en/US/technologies/tk648/tk872/technologies_white_paper0900aecd8054d37d.html

Figure 5 - http://www.tcpipguide.com/free/t_IPv6DatagramSizeMaximumTransmissionUnitMTUFragment-4.htm