A SYSTEMATIC REVIEW OF TRANSITION FROM IPV4 TO IPV6

Ordabayeva G.K.
Department of Information Systems, Kazakh National University named Al-Farabi
Almaty, Kazakhstan
Phone: +77079325785
gulzi200988@mail.ru

Othman M.
Department of Commmunication Technology and Network, University Putra Malaysia
43400 UPM Serdang, Selangor D.E., Malaysia
mothman@upm.edu.my

Kirgizbayeva B.
Information Technology and Automatization, Kazakh National Agrarian University,
Almaty, Kazakhstan
bibinur.kirgizbaeva@yandex.ru

Iztaev Zh.D.
Information Technology and Energetic Scientific school, M.Auezov South Kazakhstan State University,
Shymkent, Kazakhstan
Zhalgasbek71@mail.ru

Bayegizova A.
Department of Radio engineering, electronics and telecommunications, L.N.Gumilyov Eurasian National University,
Nur-Sultan, Kazakhstan
baegiz_a@mail.ru

ABSTRACT

Personal computers (PC) and gadgets have recently become increasingly associated with the Internet. Internet Protocol (IP) has become the driving force for a decade for which devices and organizations tend to rely as a means of communication between hosts or nodes. Thus, it becomes necessary to have a reliable Protocol that will adapt to changes.

In a network, an IP address is assigned to each interface that connects to the Internet. Addresses are still assigned using Internet Protocol version 4 (IPv4). IPv4 has demonstrated reliability, compatibility with a wide range of protocols, applications and ease of implementation. IPv4 was supposed to cover all network interfaces, but with a huge increase in the number of devices (computer, mobile phone, tablet, routers, servers and etc.), the reserve of assigned addresses will be exhausted. IPv6 has been deployed to provide new services and to support network growth. This paper compares the key IPv4 and IPv6 specifications, compares the IPv4 and IPv6 header fields and compares the header structure.

This article discusses the main problems and difficulties in the transition from IPv4 to IPv6, and describes the methods of translation and tunneling.

Keywords

IPv4, IPv6, dual stack, tunneling, translation, migrating to IPv6, IPv6 transition mechanisms.

Introduction

This era is said to be the era of computers. Every day, computers are rapidly changing our way of life. The exchange of information and data is carried out at lightning speed.

Computer networks, also called data networks, are the logical result of the evolution of two of the most important scientific and technical branches of modern civilization - computer technology and telecommunication technologies [1].

To build networks we use Internet protocols. The Internet Protocol (IP) is the principal communications protocol in the Internet protocol suite for relaying datagrams across network boundaries. Its routing function enables internetworking, and essentially establishes the Internet [2].

In essence, the terms "protocol" and "interface" express the same concept - a formalized description of the procedure for the interaction of two objects, but traditionally in the networks they were assigned different scopes: protocols determine the rules of interaction between modules of the same level in different nodes, and interfaces - rules of interaction of modules of neighboring levels in a single node. A hierarchically organized set of protocols sufficient for organizing the interaction of nodes in a network is called a protocol stack [3].

IP has the task of delivering packets from the source host to the destination host solely based on the IP addresses in the packet headers. For this purpose, IP defines packet structures that encapsulate the data to be delivered. It also defines addressing methods that are used to label the datagram with source and destination information.

Internet Protocol (IP) is a set of rules that defines how a computer sends data to another computer. Internet Protocol is working on Network Layer of Open Systems Interconnection (OSI) model and also working on Internet Layer of TCP/IP model [1, 4]. Computers and devices have a unique IP address. The usage of this is to route a packet via a network from source to destination. IP assigns unique addresses to devices across networks, encapsulates the data into datagrams and sends the datagram to its destination [5].

There are various IP version types, however IPv4 and IPv6 have become popular [6]. This document contains six sections. Section II describes the history of the development of IP technologies. Section III shows the types of TCP/IP. In section IV describes comparative analysis between IPv4 and IPv6. Section V suggests transition methods. Section VI describes the Comparative analysis and future directions conclusion. Section VII Conclusion.

II The history of the development of IP technologies

In order for information to be correctly transmitted from one computer to another, it is necessary to have unique addresses with the help of which one can unambiguously identify (identify) the recipient of information. Just as regular mail delivers postal items to addresses that include the region, city, street, house,

ICEMIS'20 (DTESI'20), September 14–16, 2020, Almaty, Kazakhstan
© 2020 Association for Computing Machinery.
ACM ISBN 978-1-4503-7736-2/20/06$15.00
https://doi.org/10.1145/3410352.3410735

apartment, and the Internet, information packets are delivered to the addresses, only the address does not indicate houses and streets, but the numbers of networks which is connected to the recipient computer and the numbers of the computers themselves on these networks.

IP (Internet Protocol, "Internet Protocol"), which forms the basis of the entire Internet, is the most prominent example of a connectionless network service. Each packet contains the destination IP address with which the router performs individual packet forwarding [7].

The data flow of the IP protocol is broken down into specific parts - datagrams and considers each datagram as an independent unit that has no connection with other datagrams. Datagram is the general name of the data unit used by the connectionless protocols. The primary purpose of the IP protocol is to transfer datagrams between networks. Often, datagrams transmitted using IP are called IP packets [8].

Network complexity grows as the result of organic expansion and network-intensive initiatives such as virtualization, cloud adoption, and bring your own device (BYOD). These factors increase the need for accurate and dynamic IP address management (IPAM). IPAM discovers IP addresses on a network, deploys new addresses, keeps accurate records, enables address planning, and monitors IP address usage from a central interface.

An IP address is the single, unique identifier for physical and virtual objects on the network.

Ranges of IP addresses define the networks themselves. Infoblox takes IP address management to a new level by providing information that gives IT departments and organizations integrated management of network resources while advancing the concept of IP resource management [9].

An IP address is a unique number that uniquely identifies a computer on the Internet. An IP address is four numbers (octets), separated by dots, for example, 194.67.67.97 (no dot after the last number). Decryption of such an address is from left to right. The first number is the number of the largest network in the Internet, the last is the number of a specific computer. The second and third numbers denote network segments, for example, a regional and local network.

Special computers, called routers, use IP addresses to send information packets in the right direction, that is, to the recipient specified in them.

For application programs, such as e-mail programs, it is necessary not only to properly package information into packages and send them, but it is also necessary to clearly agree on the contents of these packages, as well as on the procedure for exchanging packages. For example, to receive a letter, you must present the password of the mailbox owner, and this is a whole sequence of actions. Thus, other protocols are needed (Table 1).

III The types of TCP/IP

Historically, IP was the connectionless datagram service in the original Transmission Control Program introduced by Vint Cerf and Bob Kahn in 1974, which was complemented by a connection-oriented service that became the basis for the Transmission Control Protocol (TCP). The Internet protocol suite is therefore often referred to as TCP/IP [1].

In May 1974, Vint Cerf and Bob Kahn provided an article titled “A Protocol for Packet Network Intercommunication”. The paper issued by the Institute of Electrical and Electronic Engineers (IEEE) [8].

TCP defines how data transmitted over a network is divided into parts - packets and distributed to the Internet. TCP numbers each part to restore order later. To send this numbering along with the data, TCP wraps each piece of information with its cover - an envelope (TCP envelope) that contains the relevant information. The resulting TCP packet is placed in a separate IP envelope and an IP packet is obtained. Each packet is numbered and transmitted independently, therefore the paths traversed by the packets may not coincide and the sequence of their delivery to the addressee may differ from the original one. The receiver unpacks IP envelopes containing TCP envelopes, unpacks the last ones and puts the data in the required order. In the end, information is collected and fully recovered. This array is sent to the user (to disk, to screen, to print). Thus, the transfer of information via TCP/IP protocol consists of four stages:

1) TCP Protocol: splitting information into numbered packets;

2) IP protocol: packet transmission to the recipient;

3) TCP protocol on the recipient side: checking the completeness of received packets;

4) TCP protocol: recovery of the required information.

Table 1. Type of protocols

Protocol name	Decryption	Purpose
HTTP	Hyper Text Transfer Protocol	Hypertext Transfer Protocol is the set of rules for transferring files (text, graphic images, sound, video, and other multimedia files) on the World Wide Web.
FTP	File Transfer Protocol	File transfer protocol is a standard network protocol used for the transfer of computer files between a client and server on a computer network.
SMTP	Simple Mail Transfer Protocol	Simple email sending protocol is a communication protocol for electronic mail transmission
POP3	Post Office Protocol 3	Post Office Protocol 3 is the most recent version of a standard protocol for receiving e-mail.
NNTP	News Net Transfer Protocol	News Net Transfer Protocol is the protocol used to connect to Usenet servers and transfer newsgroup articles between systems over the Internet (teleconferencing protocol).

The Figure 1 is shown the TCP/IP layers [3]:

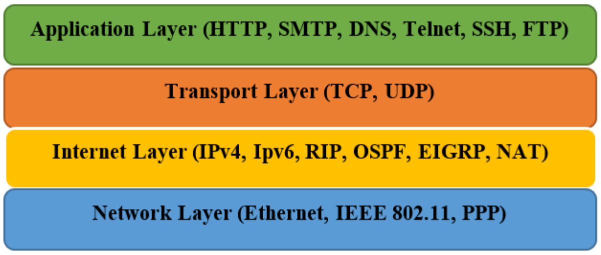

Application Layer (HTTP, SMTP, DNS, Telnet, SSH, FTP)
Transport Layer (TCP, UDP)
Internet Layer (IPv4, Ipv6, RIP, OSPF, EIGRP, NAT)
Network Layer (Ethernet, IEEE 802.11, PPP)

Figure 1. TCP/IP model [3].

The Network Layer is the foundation of a computer network, on top of which all the logic of interaction is built, the task of coding data for their transmission over the physical medium is solved. Addressing is also implemented at this level, with the help of which the switches understand - to which device which frame to send. The following protocols and technologies that work on the data link layer can be distinguished: Ethernet, IEEE 802.11 WLAN, SLIP, Token Ring, ATM.

The Internet Layer is one of the most important levels, since it is here that the IP protocol works. Also at this level, dynamic routing protocols work, the NAT protocol, which is responsible for the magic of transforming (broadcasting) private IP addresses to public ones that are routed on the Internet. This level was designed to allow interoperability between two independent networks. The main physical device on the Internet is a router, which determines where to send a packet to the IP address located in the IP packet header, the router uses masks for this, and it also uses dynamic routing protocols, with the help of which one router talks about known it IP addresses to another router.

There are a lot of network layer protocols, the most important for us at this stage is the ARP protocol, which helps determine the MAC address by a known IP address.

The Transport layer in modern computer networks is essentially represented by two protocols: TCP and UDP. TCP is mainly used to transmit text data and files over the network; UDP is used to transmit audio and video data over the network.

Transport level mechanisms are implemented on target computers, be it a server or a client, depending on the type of the end device, its operation logic at the transport level changes slightly. The computer and its operating system or a special network library on this computer are responsible for the work of the transport layer, which can be accessed by any application that wants to send or receive data.

Application Layer the main task is to provide the user with a convenient interface for interacting with computers and computer networks.

Important protocols:

• DHCP - a protocol that allows you to dynamically provide IP-addresses and other data to client machines for connecting to the network;

• DNS - allows you to convert IP addresses to domain names of sites and vice versa;

• SNMP - a protocol that is used in all systems for managing and monitoring computer networks;

• SSH is a protocol for secure remote management; when using SSH, data is encrypted;

• Telnet is a remote management protocol that implements a simple text-based network interface.

Also worth noting are the following protocols related to the application layer of the TCP/IP protocol stack model:

- RDP - protocol for remote computer control;

- SMPT, IMAP, POP3 - email protocols for the implementation of different functionalities;

- FTP and SFTP - protocols for transferring files over the network, the first uses the TCP protocol, and the second simpler uses UDP.

Application Layer cannot be distinguished by separate hardware, since the tasks of the application level are solved programmatically, and the PDU, that is, units of measurement, is simply data that may appear in one way or another, depending on the application that is running, processing or transmitting data [6,8,9].

METHODOLOGY

IV Describes comparative analysis between IPv4 and IPv6

Information technologies have penetrated into various spheres of human life. Virtually any modern process is automated and executed by a computer. The scale of ubiquitous automation continues to grow. Together with the scale of networks, the complexity of control over them is growing. The process of administration of large heterogeneous networks requires more and more resources to monitor, identify and prevent possible destructive information effects on them.

Thus, modern infrastructure needs tools that build an orderly process of monitoring, managing and reacting to deviations in the operation of large-scale networks.

IP is an address Protocol that is responsible for addressing the entire network. That is, through the use of IP Protocol, each computer (device) in the network has its own individual address (IP-address). Data are transmitted and exchanged at these addresses [5].

A. Internet Protocol version 4 (IPv4)

IPv4 is the fourth version of Internet Protocol, which is currently the main version and serves most of the Internet. The IPv4 protocol establishes the rules for the functioning of computer networks on the principle of packet exchange. Ipv4 is one of the main protocols for standardized Internet interconnection methods and is the first version that was introduced into production during the ARPANET. It provides a logical connection between different network devices, providing identification for each device.

The length of address is 32 bit which permits for 4,294,967,296 unique addresses. Each address is written in dotted decimal notation, where each decimal value of the four address byte is separated by “dots” or “periods”. The range of each byte is from 0 to 255 [5,10,11,12,65]. The Figure 2 shows the structure of an IP address [13].

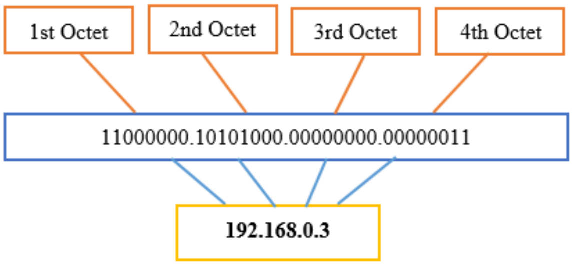


Figure 2. IPv4 Address [13].

Although we are currently running out of IPv4 addresses, some technologies have been employed to work around this issue. The most common are Network Address Translation (NAT), Classless Inter-Domain Routing (CIDR), and dynamic IPv4 address assignment (DHCP) or Dynamic Host Configuration Protocol [15]. Network Address Translation (NAT) has been the most popular of these technologies and it has helped shift further the time it would take before IPv4 addresses are exhausted [14, 16,67].

The Figure 3 shows the IP header structure and Table 2 describes IPv4 header’s fields and their functions [18].

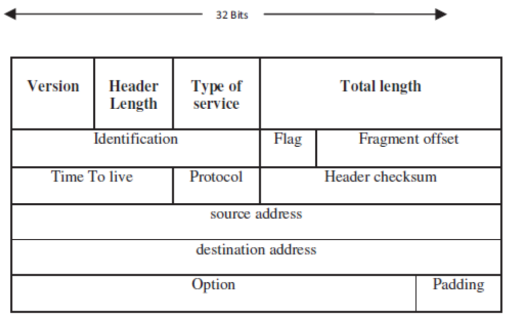


Figure 3. IPv4 header [17]

Table 2. IPv4 header's fields [17]

S.N	IPv4 Header Field	Length (bits)	Function
1.	Version	4	It defines the version of IP [1]
2.	Header Length	4	It defines the length of IP header [1]
3.	Type of service	8	It says how a datagram should be handled [16]
4.	Total Length	16	It identifies the length of Internet header and data in octet [16,17]
5.	Identification	16	It identifies the value which helps receiver to assembling the fragments of a datagram [16,17]
6.	Flags	3	It defines the IP packet can be fragmented or not [1]
7.	Fragment offset	13	It indicates the exact place of a datagram in a fragment [16]
8.	Time To live	8	It shows the maximum time a datagram is able to be in an Internet system
9.	Protocol	8	It clears up at the destination host the protocol which the packet belongs to at the next level [1]
10.	Header Checksum	16	It investigates whether the packet got error-free [1]
11.	Source Address	32	The address of sender
12.	Destination Address	32	The address of receiver
13.	Options	Variable	This field is optional. These options may contain values for options such as Security, Record Route, Time Stamp and etc [1]
14.	Padding	Variable	Padding is added at the end of a packet if it is required by header length field. Padding makes a header conform to a standard size [1]

B. Internet Protocol version 6 (IPv6)

The most important factor in implementing IPv6 is overcoming the limitations of IPv4 address resources. IPv6 offers a practically unlimited inventory of addresses from today's point of view, which is regarded as one of the critical factors for the development of future applications — the ubiquitous spread of mobile Internet, peer-to-peer applications (for example, bittorrent, gaming applications) etc [18].

IPv6 address consists of 128 bits, that is, it is 4 times longer than 32-bit IPv4 address. Like IPv4, this address can be divided into two parts: network and host. That is, not all bits in the address have the same value. Part of the bits on the left (how much depends on the prefix) denote the network, the other bits on the right – identify the device within the network. The part responsible for storing host information is called interface id). Unlike the previous version of the Protocol, IPv6 does not use subnet masks because they would be very long, but instead uses a prefix. which is written in the same slash after the address. For example, the prefix /64 means that out of 128 bits, the first 64 bits are the network, and the rest (in this case, the second 64) is the host. The prefix describes how many bits in the address are used to store network information. These numbers separated by colons ":" [19,33,40,68].

For example: 2031:0000:130F:0000:0000:09C0:876A:130B

Additionally, this address can be shortened using some rules like compressing the block of zeros to a single zero like this [16]: 2031:0:130F:0:0:9C0:876A:130B or 0000=0

Also, successive fields of zero can be represented by double colons "::", but it is only allowed once to use a double colon, so the above example will be shortened to this: 2031:0:130F::9C0:876A:130B [16].

The amazement feature of IPv6 is its header. IPv6 header is greater than IPv4 header [20]. It removed unnecessary fields. However it improves the performance. The Figure 5 has shown the structure of IPv6 header [21,33,42].

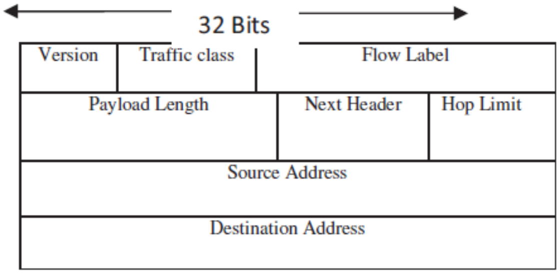


Figure 4. IPv6 header [21]

The IPv6 fixed headers, their size and meanings are described in the Table 3 [17].

The IPv6 address space will be distributed by Internet Assigned Numbers Authority (IANA) [23]. IANA will be able to redistribute the address space at any time, in case of errors in its distribution.

In addition to the obvious advantage in expanding the address space, the following advantages of IPv6 over IPv4 can be distinguished:

- ability to auto-configure IP addresses;
- simplify routing;
- simplification of the package header;
- quality of service (QoS) support);

- the availability of encryption datagrams at the Protocol level;

- increased security of data transmission [24].

In fact, almost all of the benefits of IPv6 are derived from the format of its packet and forms of addressing. The redesigned and improved standard allows to implement powerful cryptographic protection (data encryption) and many services, such as Quality of Service (QoS) at the Protocol level. QoS in IPv6 is fully supported on the network layer. This is extremely important for multimedia broadcasts. The changes made to IPv6 show that it will not only solve the main problem of the lack of address space, but will rebuild the entire structure of the Internet so that it becomes more logical and thoughtful [23, 24].

Table 3. IPv6 header's fields [17]

S.N	IPv6 Header Field	Length (bits)	Function
1.	Version	4	Indicates the version of IP. The value of this filed is 6 in IPv6 [22,]
2.	Traffic Class	8	It represents the priority or the class of the packet [22]
3.	Flow Label	20	This field indicates if this packet belongs to a sequence of packets which are sent by host [22]
4.	Payload Length	16	Gives router the length of data this packet involves in its payload [20]
5.	Next Header	8	Indicates the protocol or the type of Extension Header from upper layer [20,22]
6.	Hop Limit	8	The maximum number of links is demonstrated by Hop Limit Field that allows a packet to travel. Whenever a packet is going through a router then the number of value will be decreased by one [20]
7.	Source Address	128	Provides sender's IP address [20]
8	Destination Address	128	Provides receiver's IP address [20]

C. Internet Protocol version 10 (IPv10)

IP version 10 (IPv10) is a new version of the Internet Protocol, designed to allow IP version 6 (IPv6) (RFC-2460) to communicate with IP version 4 (IPv4) (RFC-791) and vice versa [35].

The advantages of using IPv10 [36, 37]:

1) Introduces an efficient way of communication between IPv6 hosts and IPv4 hosts;

2) Allows IPv4 only hosts to exist and communicate with IPv6 only hosts even after the depletion of the IPv4 address space;

3) Adds flexibility when making a query sent to the DNS for hostname resolution as IPv4 and IPv6 hosts can communicate with IPv4 or IPv6 DNS servers and the DNS can reply with any record it has (either an IPv6 record "Host AAAA record" or an IPv4 record "Host A record");

4) There is no need to think about migration as both IPv4 and IPv6 hosts can coexist and communicate to each other which will allow the usage of the address space of both IPv4 and IPv6 making the available number of connected hosts be bigger;

5) IPv10 support on all Internet connected hosts can be deployed in a very short time as there is no dependence on enterprise users and it is just a software development process in the NIC cards of all hosts to allow encapsulating both IPv4 and IPv6 in the same IP packet header;

6) Offers the four types of communication between hosts:

- IPv6 hosts to IPv4 hosts (6 to 4);
- IPv4 hosts to IPv6 hosts (4 to 6);
- IPv6 hosts to IPv6 hosts (6 to 6);
- IPv4 hosts to IPv4 hosts (4 to 4).

IPv10 Packet Header is shown in figure 5:

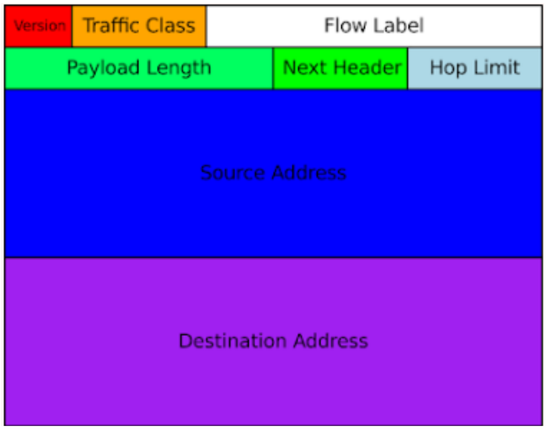


Figure 5. IPv10 Packet Header Format [36]

Important conditions for working with IPv6 [35]:

- IPv4 and IPv6 routing must be enabled on all routers, so when a router receives an IPv6 packet, it must use the appropriate routing table based on the destination address in the IPv6 packet;

- If the received IPv6 packet contains an IPv4 address in the destination address field, the router must use the IPv4 routing table to make routing decisions;

- If the received IPv6 packet contains an IPv6 address in the destination address field, the router must use the IPv6 routing table to make routing decisions;

- All hosts connected to the Internet must be IPv6 hosts to be able to communicate regardless of the IP version used.

The process of deploying IPv10 can be performed by all technology companies that develop operating systems for hosts, network devices, and security devices [36,37].

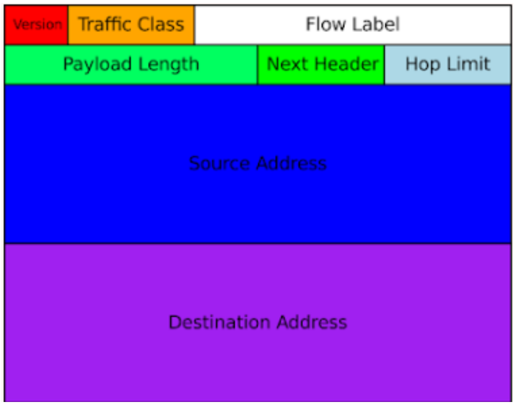


Figure 5. IPv10 Packet Header Format [36]

Important conditions for working with IPv6 [35]:

- IPv4 and IPv6 routing must be enabled on all routers, so when a router receives an IPv6 packet, it must use the appropriate routing table based on the destination address in the IPv6 packet;

- If the received IPv6 packet contains an IPv4 address in the destination address field, the router must use the IPv4 routing table to make routing decisions;

- If the received IPv6 packet contains an IPv6 address in the destination address field, the router must use the IPv6 routing table to make routing decisions;

- All hosts connected to the Internet must be IPv6 hosts to be able to communicate regardless of the IP version used.

The process of deploying IPv10 can be performed by all technology companies that develop operating systems for hosts, network devices, and security devices [36,37].

D. IPv4 / IPv6 Overview

The Regional Internet Registries (RIRs) are responsible for the regional management of Internet number resources, comprising IP addresses (IPv4 and IPv6) and Autonomous System Numbers (ASNs). The RIRs allocate, assign, and manage these resources following community-defined technical and operational policies [21].

There are five RIRs which is: the African Network Information Center (AFRINIC), American Registry for Internet Numbers (ARIN), Latin America and Caribbean Information Center (LACNIC), Reseaux IP Europeens Network Coordination Center (RIPE NCC), and Asia-Pacific Network Information Center (APNIC). Every RIR is serving a particular region of the world [22].

Each RIR community develops its own policies to manage Internet number resources, and works with other RIR communities on policies that require global coordination.

The RIRs get these Internet number resources from the Public Technical Identifiers (PTI), according to need and in line with current global numbering policy [21].

The Internet Assigned Numbers Authority (IANA) functions are a set of administrative tasks critical to ensuring the global coordination of the DNS root zone, IP addressing and protocol parameters. The IANA functions are performed by Public Technical Identifiers (PTI) under contracts and sub-contracts with the Internet Corporation for Assigned Names and Numbers (ICANN) [23].

As part of the IANA functions, PTI allocates IP address space from the pool of unallocated addresses to the RIRs according to their needs and in line with current global numbering policy. PTI also maintains a registry of the IP address blocks and Autonomous System Numbers (ASNs) that have been allocated to each RIR [73].

Each RIR makes its own requests for IP addresses and ASNs based on regional needs, and the allocations are made directly to each RIR.

The RIRs then assign IP addresses to their members, such as Internet Service Providers (ISPs), or to National Internet Registries (NIRs) [22].

Figures 6-1 and 6-9 show the Regional Internet Registries and their service areas for the IPv4 / Ipv6 protocols [23].

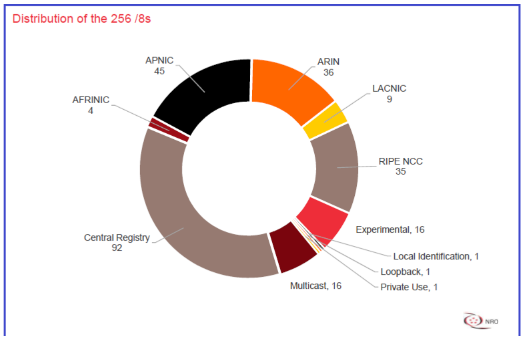
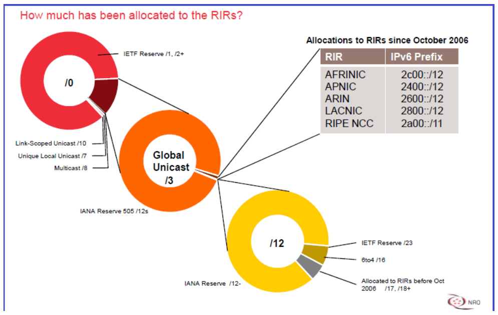


Figure 6-1. All IPv4 Address Space



Allocations to RIRs since October 2006

RIR	IPv6 Prefix
AFRINIC	2c00::/12
APNIC	2400::/12
ARIN	2600::/12
LACNIC	2800::/12
RIPE NCC	2a00::/11

Figure 6-2. All IPv6 Address Space

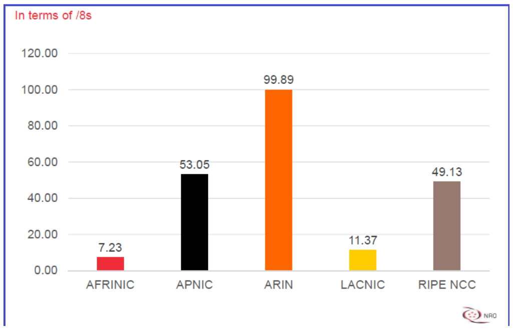


Figure 6-3. Total IPv4 Addresses Managed by each RIR

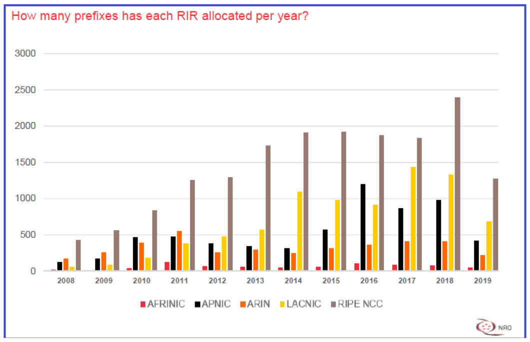


Figure 6-4. IPv6 Allocations Issued by RIRs

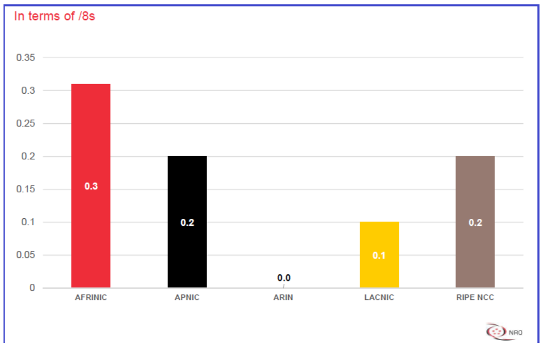


Figure 6-5. Available IPv4 Space in each RIR

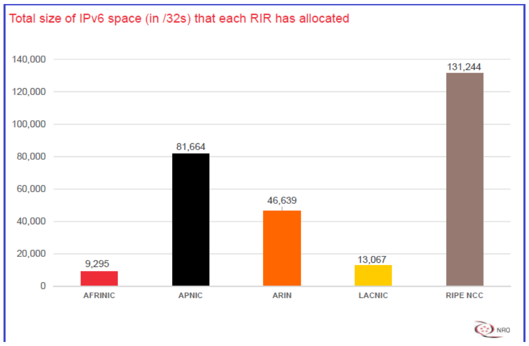


Figure 6-6. Total Allocated IPv6 Space

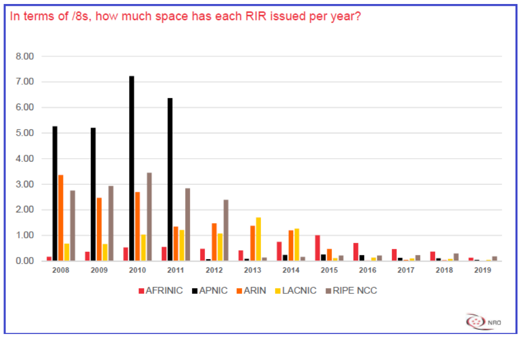


Figure 6-7. IPv4 Space issued by RIRs

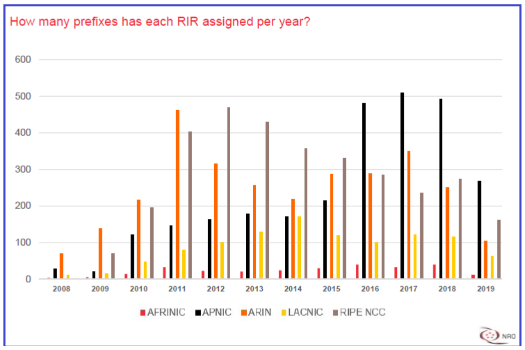


Figure 6-8. IPv6 Assignments Issued by RIRs

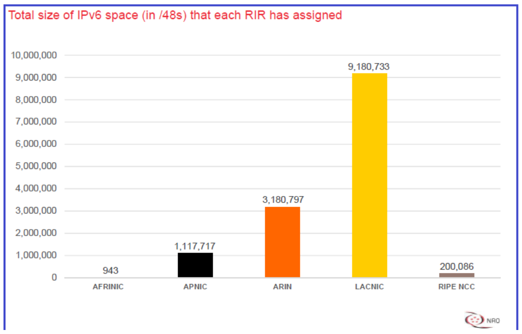


Figure 6-9. Total Assigned IPv6 Space

According to [23], the total assigned IPv6 space is:

- The APNIC currently has the total size of the IPv6 space (in/48s) assigned to each RIR 1,117,717 addresses.
- The RIPE NCC also states that the total size of the IPv6 space (in / 48s) assigned to each RIR is 200.086 addresses.
- LACNIC also states that the total size of the IPv6 space (in / 48s) assigned to each RIR is 9,180,733 addresses.
- AFRINIC also states that the total size of the IPv6 space (in / 48s) assigned to each RIR 943 address
- ARIN also states that the total size of the IPv6 space (in / 48s) assigned to each RIR is 3,180,797 addresses (Figure 7-9).

According to S.Kalwar and M.Koyuncu (2015), in IPv4, fragmentation is performed by both the sending host and the routers. In contrast, in IPv6, this is done only by the sending host. On the other hand, in the case of IPv6, it is required to protect the network from security incidents. The various differences between IPv4 and IPv6 are shown in Table 4. Also, the IP address and IP functions between IPv4 and IPv6 are compared in different concepts [59,74].

Table 4. Comparison of IPv4 and IPv6 [7]

S. N	Category	IPv4	IPv6
1.	Deployed	1981 [24]	1999 [24,51]
2.	Length of address	32 bits (4 bytes) [8]	128 bits (16 bytes) [8,52]
3.	Total number of addresses	4,294,967,296 unique addresses [10]	340,282,366,920,938,463,463,374,607,431,768,211,456 unique addresses [8]
4.	Style of address	Each IPv4 address is represented in four sets decimal digit, which is divided by dots (“.”). Such as 192.168.10.3, and the limited area of each set is from “0” to “255”.If all digits in each set is zero, we use single zero, for example 192.168.0.0 [10,13,25,54]	IPv6 address is represented in eight hexadecimal digit sets, which is divided by colons (“:”). For instance FA90:0000:0000:0000:0301:B3EE:FE1E:8009, If all digits in each set is zero, we put only a double colon. For example FA90::0301:B3EE:FE1E:8009 [11,13,25,53,54]
5.	Type of addresses	Broadcast: the packet is sent to all the interfaces (hosts) [3]. Unicast: the packet is sent to only	Multicast: the packet is sent to a number of interfaces [24] unicast: the packet is sent to only

		one interface [31]. Multicast: the packet is sent to some specific interfaces [31,55].	an interface [24]. Anycast: in this case, a number of interfaces is defined as destinations but the packet is transferred to one of the interfaces which are in set, it depends on routing protocol [55].
6.	Address Resolution Protocol (ARP)	ARP finds physical addresses, like the MAC or link address, which is associated by an IPv4 address [6]	ARP is substituted with a function of Neighbor Discovery Protocol using IMCPv6 to gain the MAC addresses [24,6]
7.	Communications trace	The task of communications trace is gathering the information of trace of TCP/IP packets which have been entered or leaved [57].	same in IPv6 [6]
8.	Configuration	IP address is configured by either DHCP or manually [45,62]	Auto configuration is one of the important features of IPv6. It is known as “plug & play” which allows a node to configure its address by itself. There are two ways of autoconfiguration in IPv6: (1). The stateless autoconfiguration: in this case the address of host doesn’t have to be configured manually, and sometimes routers need minimal configuration (2). The stateful autoconfiguration: this kind of autoconfiguration is equivalent to the DHCP protocol of IPv4. Here a host gets the IP addresses of its interfaces through a DHCPv6 server that is a pool of addresses which allocated to the interfaces. Auto-configuration is easier and more manageable for large installations [25,45,62].
9.	Domain Name Service (DNS)	For mapping the name of hosts to the IPv4 addresses and reverse, it uses host address (A) resource records in DNS [26,58].	For mapping the name of host to the addresses of IPv4 and reverse, it uses host address (AAAA) resource records in DNS [26,27,58].
10.	File Transfer Protocol (FTP)	FTP lets you to send and receive information through the network [6,60]	FTP doesn’t support IPv6 [6,60]
11.	Internet Control Message Protocol (ICMP)	Network devices use ICMP to send error messages, for example ICMP destination unreachable messages, and informational messages, like ICMP echo request and reply messages [27,47]	It is used similarly by IPv4; although, ICMPv6 has some more sufficient attributes, such as error reporting in packet processing, diagnostic activities, Neighbor Discovery process and IPv6 multicast membership reporting [27,63]
12.	Router Discovery	ICMP Router Discovery allows hosts to define the default gateway router to reach devices on different networks, it is important to note that it is optional [28]	ICMPv6 Router Solicitation and Router Advertisement messages work instead of ICMP Router Discovery. It is required [6]
13.	Routing protocols	RIP,RIP-2,IGRP,EIGRP,OSPF-2,OSPF-3,MOSPF,IS-IS,DVMRP,PIM,EGP,BGP-4 [29,47,48,65]	RIPng,OSPF-3,EIGRP,IS-IS,PIM,BGP-4 [29,47,48,65]
14.	Quality of Service	QoS lets you to demand packet bandwidth and priority for TCP/IP application [30]. In other word, QoS is a mechanism to transfer a multimedia packet such as music, voice and video with good quality but in IPv4 there isn’t any assurance that all QoS compliant devices are compatible with another device [31]	In Ipv6 there is a field which is known as Flow Label field. This field defines how specific packets are identified as well as carried by the routers. The Flow Label field lets the packets which begin from a specific host to a particular destination to be identified and handled by the routers [31]. The purpose of QoS

			mechanisms are [24]: - Real time application. - Less latence and "jitter". - More tolerance to packet losses. - Retransmissions are less important. - More importance of the temporal relationship.
15.	Security	Security is bounded to tunnelling between two networks [44,64]	IPv6 provides data security, which involves end-to-end backing for user authentication, data encryption and data integrity [44,64]
16.	IPSec support	Optional [32,64]	One of the important protocols in IPv6 is IPSec. It involves a set of cryptographic protocols for making secure communication and key exchange. The major protocols used are: (1) Authentication Header (AH) Protocol: it enables authentication and integrity of data. (2) Encapsulating Security Payload (ESP): ESP enables authentication, integrity of data and privacy of data .(3) Internet Key Exchange (IKE): this protocol sets up the security between two end points and holds the track of information therefore the communication will be secured until the end [32,66]

V Transition methods

The following mechanisms have been proposed to ensure the smooth operation of IP protocols and transition from IPv4 to IPv6 protocol: Dual stack, Tunnelling and Translation (Protocol broadcast) [10,69].

A. Dual stack

The Dual Stack (DS) transition method [43], but with the requirements that the two communicating hosts and the network between them have to support a common version of the IP protocol, and because of the IPv4 exhaustion, there is not enough IPv4 addresses to use this solution. The communicating hosts need both version of the IP addresses and it is almost impossible to provide enough public IPv4 addresses for the clients.

It is the most widely used transition techniques as it is simple to implement and is supported by mostly all operating systems [14]. In Dual Stack both IPv4 and IPv6 protocols work in parallel however the IPv6 network is implemented on an existing IPv4 network. This method is common for businesses who are looking to slowly convert their existing IPv4 devices to IPv6 [11,15, 19].

Figure 7 shows the variation in a IPv4 only stack and dual stack [43].

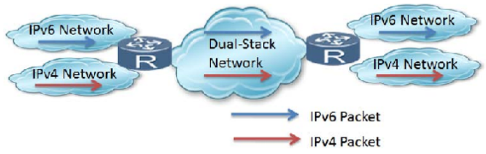


Figure 7. Dual Stack Protocol [43]

Dual stack implementation in IPv4 and IPv6 was evaluated by Khalid EL K. et al. [48].

In the article by Zhiwei Yan, an in-depth analysis of three types of standardized mobility management protocols with support for two stacks. Due to differences in the basic protocols, their separate extensions with two stacks have different functions and are thus suitable for deployment in different scenarios and stages of the evolution of mobile Internet [39].

All microsofts desktops and servers, systems supported by Linux and its different variations, Cisco IOS and Cisco routers support dual stack environment [13].

B. Tunnelling

Tunneling is intended for communication between IPv6 nodes or networks through an existing data transmission medium that supports only a version of the IPv4 protocol. Between networks or hosts working with IPv6 using a special software creates a "tunnel". Packets of information getting on one end of this "tunnel" are being converted. This conversion is by encapsulating IPv6 packets into IPv4 standard packets, which are then are sent to the "exit". At the second end of the "tunnel" is the reverse process. IPv4 packets are extracted from IPv4 packets, which then processed by routers as usual [15,18,19,38,72].

Tunnelling can be either manual or automatic and it replaces either TCP or UDP protocol at layer four (transport layer). Figure 8 shows the Tunnelling concept [11].

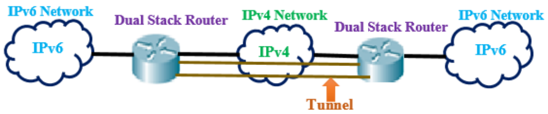


Figure 8. Tunnelling concept [11]

The main advantage of this mechanism is the lack the need to purchase and install additional software ensure each node. So, for an IPv6-based network, it is enough to create several "tunnels" connecting it with other such networks [16]. Tunneling methods are given in Table 5 [16,18,19,38,70].

Table 5. Tunneling methods [16,18,19,38,41,70]

Method name	Characteristic
6in4	One of the oldest tunneling methods developed in 1996 year, and to this day highly recognized. Such large tunnel brokers like Hurricane Electric, gogo6 and SIXXS use it. Uses protocol 41 and does not work through NAT. Supported by all modern OS
6over4	According to the essence, it cannot be described as a tunnel in a normal meaning of this phrase. It uses IPv4 as a virtual ethernet for IPv6, for example, the multicast address ff02 :: 1 turns into an IPv4 multicast address 239.192.0.1. The protocol supports the generation of Link-Local addresses, Neighbor Discovery and configured automatically. Due to the fact that all routers in networks must support Multicast, the protocol has not become popular. Support in the current OS is missing or limited.
6to4	6to4 will turn your IPv4 address into an IPv6 / 48 subnet. In fact, this is the same 6in4, but with a fixed anycast IPv4 address: 192.88.99.1. The protocol is fully auto-configurable, manual configuration is not possible. Easy to configure. The disadvantage is that your IPv4 address can be obtained from the IPv6 address, and that you cannot select the server through which tunneling takes place. In some cases, you generally won't know who owns this server. Uses special prefix 2002 :: / 16. Does not work through NAT.
6rd	This protocol is based on 6to4, only intended for deployment inside a large organization or ISP. Does not use the prefix 2002 :: / 16, but uses the usual address range given to your provider. It can be automatically configured in different ways, the most popular is through DHCPv4 with a special parameter.
AYIYA	It stands for Anything In Anything, this protocol can encapsulate, in fact, something into something. The protocol is invented by the SIXXS tunnel broker and is used by him. Currently, IPv4-UDP-AYIYA-IPv6 is mainly used. There is support for cheksumm and authorization. Works through NAT.
ISATAP	This protocol is somewhat similar to 6over4, but does not use Multicast. ISATAP does not support Multicast at all. IPv6 addresses are generated based on IPv4 addresses. It is assumed that the IPv4 address will be unique, therefore it does not work with NAT. Communication with ISATAP hosts is only possible if you also have ISATAP configured. Supported by modern OS.
Teredo	Extremely popular tunneling method that does not require special settings. On Windows (starting with Vista) it is configured and enabled by default, on Linux it rises in a few seconds using Miredo. You are required to specify the Teredo server (or use the default server), everything else is configured automatically. It works through NAT, however, with nuances (it depends on the type of NAT, and on the implementation on the side of the Teredo server).
6a44	The protocol is made under the influence of Teredo, but it is intended for deployment by means of ISP. Similar to 6rd and 6to4, customers are given an IPv6 provider prefix, not a Teredo IPv6 prefix. It looks like it is not supported anywhere.
6bed4	Peer-to-Peer IPv6 on Any Internetwork. 6bed4 is designed to create a p2p IPv6 network within an IPv4 network that does not prohibit p2p connections between hosts. The protocol is a hybrid of 6to4 and Teredo: an IPv6 address is formed from an IPv4 and UDP port, if a p2p connection is not possible, a relay is used, which can be started by an ISP or simply by a third-party organization. It works through NAT, supports both autoconfiguration and manual configuration.
Lisp	The Locator / ID Separation Protocol aims to separate the dependence of the IPv6 address on the client's location. Using this protocol, you can use your (suppose home) IPv6 address outside your network, without traffic proxying. By concept, similar to Proxy Mobile IPv6. The protocol itself is quite complicated and using it exclusively for tunneling is rather silly. Does not work through NAT. Supported by Cisco, Linux and FreeBSD.
SEAL	Subnetwork Encapsulation and Adaptation Layer. A completely new protocol, draft appeared in October 2013. It supports several IPv4 links, and, accordingly, multihoming. There is an authentication and anti-replay mechanism. SEAL Control Message Protocol is used to exchange service data between hosts.

C. Translation (Protocol broadcast)

The two mechanisms discussed above for the interaction of the two protocols — double stack and tunneling — rely on the host to support at least the IPv6 protocol or even both. However, in some cases, a host that works only with IPv6 needs to communicate with a host that works only with IPv4. For this, there is a third mechanism - a mechanism that converts IPv6 packet headers into IPv4 headers and back [56].

A software or hardware gateway, bridge, switch or router can act as a broadcasting element.

The most well-known translation method is NAT64, which allows IPv6 devices to work with IPv4 devices. However, this scheme has one feature - the need for additional support for the DNS domain name system, one of the most critical Internet applications. After all, when accessing a website or sending e-mail, DNS takes on the task of translating the name to the IP digital address (whether IPv4 or IPv6). Especially for the translation mechanism, DNS64 was developed, which replaces the IPv4 address in the DNS response to the synthesized IPv6 address, which is understandable to both the client and the NAT64 protocol translator [71].

Network Address Translation 64 (NAT64) allows devices running IPv6 to communicate with devices running IPv4 using a translation method similar to the NAT from IPv4 translation method. An IPv6 packet is converted to an IPv4 packet and vice versa [19] (figure 9).

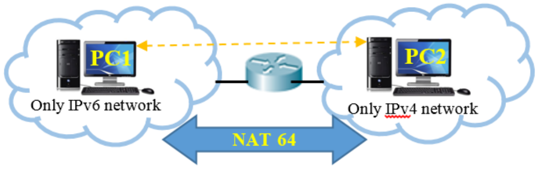


Figure 9. Translation (Protocol broadcast) [19]

VI Comparative analysis

This part is an overview of existing random access methods according to the proposed classification. This section analyzes and compares the effectiveness of these methods according to the results presented in each paper.

For network modeling, we used the Riverbed Modeler program, which allows you to create network models and obtain characteristics in the form of graphs: packet delay time, throughput at the node, and server load.

Specifications were set for generating traffic according to a certain law and with an intensity of 100 packets per second from the connected device (figure 10). Each network element was assigned an individual IP address. Initially, the network was configured over IPv4, then the workstations and routers were reconfigured to work over IPv6.

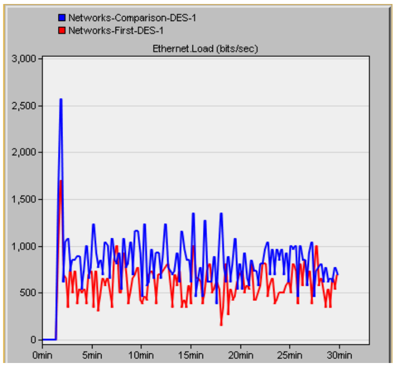


Figure 10. Traffic at the server entrance (X-axis-time in minutes, Y-load in bits/sec)

The comparison graph in figure 11 shows, that there are no significant differences in Ethernet delay. Unlike server load, which has increased, network delay has not changed.

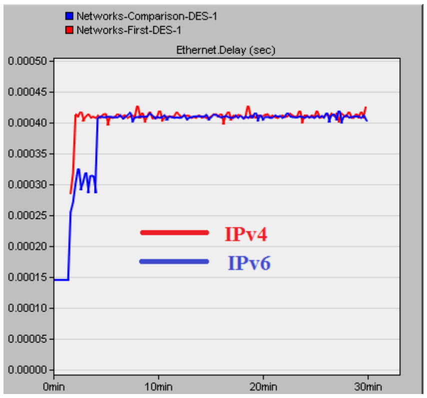


Figure 11. The Ethernet delay (sec)

By running a simulation of the network for a duration of 30 minutes, the results of the studied characteristics were obtained. As a criterion for evaluating network performance, the average time spent by a packet in a network with multiple switching nodes connected by duplex communication lines with a bandwidth of $d_{k,l}$ bytes/s between k and l nodes is used [75].

Each switching node has a buffer of unlimited capacity, and the average packet length is $L_p=1/\mu$ bytes. The data stream originating at node i and intended for node j is the simplest with an average intensity of $\lambda_{i,j}$ packets/s. The total average network intensity is determined by the formula:

$$\lambda = \sum_{i=1}^{N}\sum_{j=1}^{N}\lambda_{ij} \qquad (1)$$

Where, N - is the total number of node switches.

The expression for the average packet delay looks like this:

$$T = \frac{1}{\lambda}\sum_{k=1}^{N}\sum_{j=1}^{N}\gamma_{kl}t_{kl} \qquad (2)$$

Where, t_{kl} - average time of messages stay in the line,

$$\gamma_{kl} = \sum_{i=1}^{N}\sum_{j=1}^{N}\lambda_{ij}x_{kl}^{(i,j)} \qquad (3)$$

Where, $x_{kl}^{(i,j)}$ - the percentage of flow that passes along the line (k,l)

The comparison graph of IPv4 and IPv6 protocols shows the dependence of packet delay time on network size. Based on this comparative characteristic, we can conclude that the use of the IPv6 protocol with an increase in network size gives an advantage over IPv4. As a result, the time average (in Ethernet delay (sec)) in IPv6 decreased by 9.5% (fig. 12).

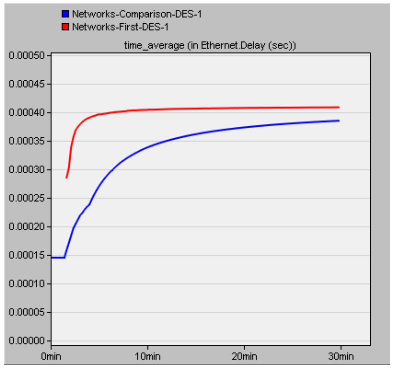


Figure 12. The time average (in Ethernet delay (sec))

In this section, we focused on the available materials according to IEEE standards, Springer and Google. About 150 scientific documents were analyzed, including journals, conference reports, PhD theses and books. We compared the number of citations based on the 138 articles. Related documents cover more than 5,703 citations from 2000 to 2019. We have identified which transition type has the most references in this area. We have classified these items into four main categories, including "IPv6", " IPv4/IPv6", "Dual stack" and "Tunneling" (Table 6).

Figure 13-1 shows that the largest number of articles are written on the topic "IPv4/IPv6" from 2010 to 2014 and from 2015 to 2019, while "IPv6" have the largest number of articles from 2010 to 2014. The Figure 13-1 also shows that "Dual Stack" has the largest number of articles from 2015 to 2019. In addition, the figure shows that the largest number of articles were published between 2010 and 2014. Similarly, Figure 13-2 gives some information about number of citations to documents from 2000 to 2019.

The figure indicates that the articles published from 2000 to 2004 and from 2010 to 2014 in the "IPv4/IPv6" category have the largest number of citations.

Table 6: Typology of research in transition IPv4 to IPv6

Groups	Objective	The number of papers	The number of citations
IPv6	Standards, Conference articles, PhD theses, book	38	2155
IPv4/IPv6	Standards, Conference articles, Patents, PhD theses	48	2908
Dual stack	Conference articles	28	1410
Tunneling	Standards, Conference articles	22	1042

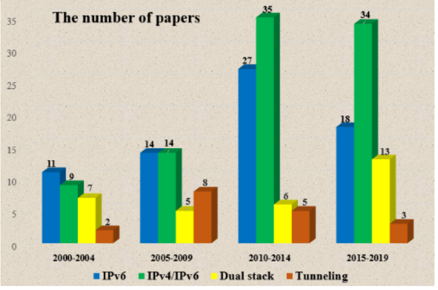


Figure 13-1. The number of papers

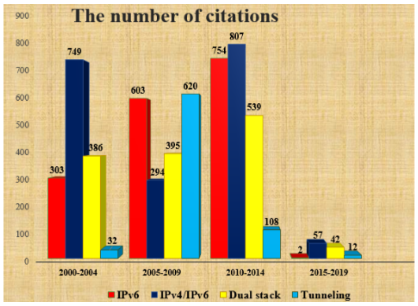


Figure 13-2. The number of citations

Figure 13. Comparison and typology of the researches

According to [76] the following graphs show the evolution of default protocol, v6 address types, and average bandwidth in Kazakhstan over time. They are generated using the data collected by the ipv6-test.com connection test page, and are updated on a monthly basis (fig.14-1, 14-2).

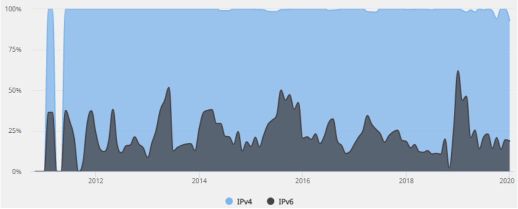


Figure 14-1. Overall IPv6 and v4 protocol support in Kazakhstan

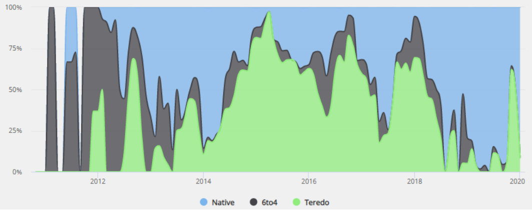


Figure 14-2. IPv6 address types in Kazakhstan

Here you can see the evolution of address types over time, and measure usage of 6to4 and Teredo tunneled connectivity.

It should be noted that because 6rd works with native addresses, it cannot be detected here as tunneled. This is also the case with VPN based tunnels.

VII Conclusion

In this paper, we compared IPv4 and IPv6 in the address structure, header structure, header fields, security, routing protocols, IP address configuration, functions of various protocols, etc.

IPv4 is the first version of IP to be used worldwide. When IPv4 was developed, it was estimated that it should be used for a long time, but the number of devices that can connect to the network is increasing, so IPv4 ran into some problems.

In this research, we found the main disadvantages of IPv4 and the main features of IPv6 that address the disadvantages of IPv4. Lack of addresses is one of the important IP problems, people use several devices, such as PCs, laptops, PDAs and telephones, so the request for IP addresses is growing, so the number of IPv4 addresses will be a problem in the future.

IPv6 provides more address space, the IPv4 address length is 32-bit, it increases to 128-bit in IPv6. The security field (IPsec) in IPv4 is optional, and all security responsibility lies with endpoints that are not secure. The IPv6 header contains the IPsec field, and it is required. In IPv4, IP configuration is manual or DHCP, but IPv6 simplifies configuration using automatic configuration. According to previous analyzes, IPv6 will be better than IPv4. As the next generation Internet Protocol, IPv6 provides several features to address IPv4 restrictions [49,50].

The transition process is dependent on ISPs to begin the deployment and provision of an IPv6 connection through their access networks. The IETF has proposed many mechanisms to begin a smooth transition to IPv6. These mechanisms are dual stack, tunneling and translation.

REFERENCES

[1] Olifer V.G., etc. Computer networks. Principles, technologies, protocols. – SPb.; 2016.

[2] Murray, D. (2015) Why internet protocols need incentives. In: 2015 IEEE 29th International Conference on Advanced Information Networking and Applications Workshops (WAINA), 24-27 March 2015, Gwangiu, South Korea

[3] “IPv4 – Tutorial”, Tutorialspoint, [Online], Available: https://www.tutorialspoint.com/ipv4/ipv4_overview.htm [Accessed By 19 July 2019].

[4] El Khadiri, K., El Kamoun, N., Labouidya, O., & Hilal, R. (2018). LISP: A Novel Solution For The Transition From IPv4 to IPv6. INTERNATIONAL JOURNAL OF COMPUTER SCIENCE AND NETWORK SECURITY, 18(10), 130-139.

[5] Tadayoni, R., & Henten, A. (2016). From IPv4 to IPv6: Lost in translation? Telematics and Informatics, 33(2), 650–659. http://dx.doi.org/10.1016/j.tele.2015.10.004

[6] “Comparison of IPv4 and IPv6” [Online], Available: http://www.ripn.net/articles/IPv6_transition [Accessed by 24 July 2019]

[7] A. Shiranzaei and R.Z. Khan, "A Comparative Study on IPv4 and IPv6" International Journal of Advanced Information Science and Technology (IJAIST) ISSN: 2319:2682 Vol.4, No.1, January 2015 DOI:10.15693/ijaist/2015.v4i1.9-16

[8] “IPv6 theory and practice: introduction to IPv6” [Online], Available:https://habr.com/ru/post/210100 [Accessed by 24 July 2019]

[9] “The Benefits Of IPv6”, [Online], Available: http://www.ipv6.ru/russian/history/ipv6.php [Accessed By 24 July 2019]

[10] Digvijay Dhamale and etc. Migration from IPv4 to IPv6. International Journal of Pure and Applied Mathematics. Volume 118 No.24 2018, p.1-9

[11] Yashwin Sookun, Vandana Bassoo. Performance Analysis of IPv4/IPv6 Transition Techniques. IEEE International Conference on Emerging Technologies and Innovative Business Practices for the Transformation of Societies (EmergiTech) 2016, 978-1-5090-0706-6/16/$31.00

[12] Pujol, E., Richter, P., & Feldmann, A. (2017). Understanding the share of IPv6 traffic in a dual-stack ISP. In M. Kaafar, S. Uhlig, & J. Amann (Eds.). Passi+ve and active measurement. PAM 2017 (pp. 3–16). Cham: Springer.

[13] Sheetal Singalar, R.M.Banakar. Performance Analysis of IPv4 to IPv6 Transition Mechanisms, IEEE, 2018. 978-1-5386-5257-2/18/$31.00.

[14] A. Quintero, F. Sans and E. Gamess, "Performance Evaluation of IPv4/IPv6 Transition Mechanisms," International Journal of Computer Network and Information Security, vol. 8, (2), pp. 1, 2016.

[15] Pyung Soo Kim, “Analysis and Comparison of Tunneling based IPv6 Transition Mechanisms,” International Journal of Applied Engineering Research ISSN 0973-4562 Volume 12, Number 6, 2017, pp. 1-4.

[16] Adira Quintero, Francisco Sans, Eric Gamess, “Performance Evaluation of IPv4/IPv6 Transition Mechanisms,” I. J. Computer Network and Information Security, 2016, pp. 1-5.

[17] Manal M. Alhassoun, Sara R. Alghunaim, “A Survey of IPv6 Deployment,” (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 7, No. 9, 2016, pp.1-5.

[18] “All IPv6 Tunneling Technologies in Clear Language”, [Online], Available: https://habr.com/ru/post/207562 / [Accessed By 27 July 2019]

[19] Robachevsky A. From the life of IP addresses. Outlook for IPv4 and the transition to IPv6 addressing. [Electronic resource] - Access mode. - URL: http://www.ripn.net/articles/IPv6_transition/ (appeal date 07/27/2019).

[20] ICANN (2017). ICANN's IPv6 Initiative. available at https://www.icann.org/resources/pages/ipv6-initiative-2017-02-28-en (accessed 08 August 2019)

[21] A. Shiranzaei, And R. Z. Khan, “Internet protocol versions-a review,” proceeding of the 9th INDIACom; 2015 2nd International Conference on Computing for Sustainable Global Development, in press.

[22] “PTI and the IANA Functions”, [Online], Available: https://www.nro.net/internet-governance/iana/ [Accessed By 01 August 2019]

[23] Internet Number Resource Report. Prepared by Regional Internet Registries AFRINIC, APNIC, ARIN, LACNIC, RIPE NCC– Q2 As of 30 June 2019

[24] Taniya Jain, Vedansh Gupta, Mahendra singh Sagar (2018) “Role and Issues of IPV4 and IPV6” International Conference on Advanced Computing (ICAC-2018) College of Computing Sciences and Information Technology (CCSIT) ,Teerthanker Mahaveer University , Moradabad, pp.233-242.

[25] S.Pachori.,”Ipv4 vs Ipv6 comparison“ [Online], Available: https://www.slideshare.net/ shaileshpachori/ master-all-home [Accessed By 01 August 2019]

[26] Pickard, J., Angolia, M., & Drummond, D. (2019). IPv6 Diffusion Milestones: Assessing the Quantity and Quality of Adoption. Journal of International Technology and Information Management, 28(1), 2-28.

[27] S.V.Tagliacane, P.W.C. Prasad, G.Zajko, A.Elchouemi, Ashutosh Kumar Singh. Network Simulations and future technologies in teaching Networking Courses. IEEE WiSPNET 2016 conference, pp.644-649

[28] Sheetal Singalar, R M Banakar. Performance Analysis of IPv4 to IPv6 Transition Mechanisms. 2018 Fourth International Conference on Computing Communication Control and Automation (ICCUBEA)

[29] C.G.Dumitrache, G.Predusca, L.D.Circiumarescu, N.Angelescu, D.C.Puchianu. Comparative study of RIP, OSPF and EIGRP protocols using Cisco Packet Tracer. 978-1-5386-2059-5/17/$31.00 ©2017 European Union

[30] H. Al-Fayyadh and M. Koyuncu, "Comparison of QoS architectures for VoIP traffics in IPv4 and IPv6", IEEE 10th International Conference on Application of Information and Communication Technologies (AICT), Baku, 2016, pp. 1-5.

[31] “Top 10 features that make IPv6 'greater' than IPv4,” K. Das, IPv6.com, [Online], Available: https://www.ipv6.com/general/top-10-features-that-make-ipv6-greater-than-ipv4/ [Accessed By 01 August 2019].

[32] Inforzato et al. SCIP AND IPSEC OVER NAT / PAT ROUTERS. United States Patent Application Publication. Pub . No . : US 2019 / 0097968 A1. Pub . Date : Mar . 28, 2019

[33] Requirements for IPv6 Routers draft-ali-ipv6rtr-reqs-02. [Online], Available: https://tools.ietf.org/html/draft-ali-ipv6rtr-reqs-02 [Accessed By 24 July 2019]

[34] “Best Practices for Successful IP Address Management (IPAM)” [Online], Available: https://info.infoblox.com/resources-whitepapers-best-practices-successful-ip-address-management-ipam [Accessed By 04 August 2019].

[35] “Internet Protocol version 10 (IPv10)” [Online], Available: http://internetprotocolv10.blogspot.com/2014/08/internet-protocol-version-10-ipv10-v.html [Accessed By 04 August 2019].

[36] “Internet Protocol version 10 (IPv10) Specification draft-omar-ipv10-11”)” [Online, Available: https://tools.ietf.org/html/draft-omar-ipv10-11 [Accessed By 04 August 2019].

[37] “Internet Protocol version 10 (IPv10)” [Online, Available: https://www.youtube.com/watch?v=PU5K7LhZghk [Accessed By 04 August 2019].

[38] Dipti Chauhan, Jay Kumar Jain, Sanjay Sharma, "An end-to-end header compression for multihop IPv6 tunnels with varying bandwidth", Eco-friendly Computing and Communication Systems (ICECCS) 2016 Fifth International Conference on, pp. 84-88, 2016.

[39] Zhiwei Yan, Hwang-Cheng Wang, Yong-Jin Park, Xiaodong Lee, "Performance study of the dual-stack mobile IP protocols in the evolving mobile internet", Networks IET, vol. 4, no. 1, pp. 74-81, 2015.

[40] Jonne Soininen, Jouni Korhonen, "Survey of IPv6 Support in 3GPP Specifications and Implementations", Communications Surveys & Tutorials IEEE, vol. 17, no. 3, pp. 1634-1648, 2015.

[41] Jia-Jhun Lin, Kai-Ching Wang, Shin-Ming Cheng, Yen-Chun Liu, "On exploiting SDN to facilitate IPv4/IPv6 coexistence and transition", Dependable and Secure Computing 2017 IEEE Conference on, pp. 473-474, 2017.

[42] Cong Liu, Yong Cui, Chaokun Zhang, Jianping Wu, "Generic application layer protocol translation for IPv4/IPv6 transition", Communications (ICC) 2017 IEEE International Conference on, pp. 1-6, 2017.

[43] Ummi Suraya Shaharuddin, Ruhani Ab Rahman, Murizah Kassim, Mat Ikram Yusof, "Performance comparison of Multimedia Applications over IPv4 and IPv6 Dual Stack technology", System Engineering and Technology (ICSET) 2016 6th International Conference on, pp. 1-6, 2016.

[44] Tao Chen, Haiping Huang, Zhengyu Chen, Yiming Wu, Hao Jiang, "A Secure Routing Mechanism against Wormhole Attack in IPv6-Based Wireless Sensor Networks", Parallel Architectures Algorithms and Programming (PAAP) 2015 Seventh International Symposium on, pp. 110-115, 2015.

[45] Yong Cui, Yuchi Chen, Jiangchuan Liu, Yiu-leung Lee, Jianping Wu, Xingwei Wang, "State management in IPv4 to IPv6 transition", Network IEEE, vol. 29, no. 6, pp. 48-53, 2015.

[46] Pickard, J., Southworth, J., & Drummond, D. (2017). The IPv6 Internet: An assessment of adoption and quality of services. Journal of International Technology and Information Management, 26(2), 48–64.

[47] **[88]** El Khadiri, K., Labouidya, O., El Kamoun, N., & Hilal, R. (2018, October). Study of the Impact of Routing on the Performance of IPv4/IPv6 Transition Mechanisms. In International Conference on Advanced Information Technology, Services and Systems (pp. 43-51). Springer, Cham.

[48] El Khadiri, K., Labouidya, O., Elkamoun, N., & Hilal, R. (2018). Performance evaluation of IPv4/IPv6 transition mechanisms for real-time applications using OPNET modeler. Performance Evaluation, 9(4).

[49] El Khadiri, K., Labouidya, O., Elkamoun, N., & Hilal, R. (2018). Performance analysis of video conferencing over various IPv4/IPv6 transition mechanisms. IJCSNS, 18(7), 83-88.

[50] Al Farizky, R. F. (2017, August). Routing protocol RIPng, OSPFv3, and EIGRP on IPv6 for video streaming services. In 2017 5th International Conference on Cyber and IT Service Management (CITSM) (pp. 1-6). IEEE.

[51] Samad, F., Abbasi, A., Memon, Z. A., Aziz, A., & Rahman, A. (2018). The future of internet: IPv6 fulfilling the routing needs in internet of things. International Journal of Future Generation Communication and Networking, 11(1), 13-22.

[52] Carisimo, E., Selmo, C., Alvarez-Hamelin, J. I., & Dhamdhere, A. (2019). Studying the evolution of content providers in IPv4 and IPv6 internet cores. Computer Communications.

[53] Samaan, S. S. (2018). Performance evaluation of RIPng, EIGRPv6 and OSPFv3 for real time applications. Journal of Engineering, 24(1), 111-122.

[54] Ashraf, Z., & Yousaf, M. (2017). Optimized routing information exchange in hybrid IPv4-IPv6 network using OSPFV3 & EIGRPv6. INTERNATIONAL JOURNAL OF ADVANCED COMPUTER SCIENCE AND APPLICATIONS, 8(4), 220-229.

[55] Ashraf, Z., & Yousaf, M. (2018, November). Optimized Convergence of OSPFv3 in Large Scale Hybrid IPv4-IPv6 Network. In 2018 14th International Conference on Emerging Technologies (ICET) (pp. 1-6). IEEE.

[56] EL KHADIRI, K., Labouidya, O., Elkamoun, N., & Hilal, R. (2018, October). Comparative Study Between Dynamic IPv6 Routing Protocols of Distance Vectors and Link States. In 2018 6th International Conference on Wireless Networks and Mobile Communications (WINCOM) (pp. 1-6). IEEE.

[57] Hilal, R. (2019). Study of the Impact of Routing on the Performance of IPv4/IPv6 Transition Mechanisms. Smart Data and Computational Intelligence, 66, 43.

[58] Hossain, M. A., & Akter, M. S. (2019). Study and Optimized Simulation of OSPFv3 Routing Protocol in IPv6 Network. Global Journal of Computer Science and Technology.

[59] Kalwar, S., Bohra, N., & Memon, A. A. (2015, February). A survey of transition mechanisms from IPv4 to IPv6 - Simulated test bed and analysis. In 2015 Third International Conference on Digital Information, Networking, and Wireless Communications (DINWC) (pp. 30-34). IEEE.

[60] Sirika, S., & Mahajan, S. (2016). Survey on dynamic routing protocols. International Journal of Engineering Research & Technology, 5(1), 10-14.

[61] Mandl P. (2019) Routing und Forwarding. In: Internet Internals. Springer Vieweg, Wiesbaden, https://doi.org/10.1007/978-3-658-23536-9_5

[62] Carisimo, E., Selmo, C., Alvarez-Hamelin, J. I., & Dhamdhere, A. (2019). Studying the evolution of content providers in IPv4 and IPv6 internet cores. Computer Communications.

[63] Haider, F., Chaudary, M. H., Naveed, M. S., & Asif, M. (2019, February). IPv6 QoS for Multimedia Applications: A Performance Analysis. In Proceedings of the 2019 8th International Conference on Software and Computer Applications (pp. 501-504). ACM.

[64] Thiruvasagam, P., George, K. J., Arumugam, S., & Prasad, A. R. (2019). IPSec: Performance Analysis in IPv4 and IPv6. Journal of ICT Standardization, 7(1), 61-80.

[65] Livadariu, I., Elmokashfi, A., & Dhamdhere, A. (2017). On IPv4 transfer markets: Analyzing reported transfers and inferring transfers in the wild. Computer Communications, 111, 105–119. http://dx.doi.org/10.1016/j.comcom.2017.07.012

[66] Šimon, M., & Huraj, L. (2019, April). A Study of DDoS Reflection Attack on Internet of Things in IPv4/IPv6 Networks. In Computer Science On-line Conference (pp. 109-118). Springer, Cham.

[67] Hammer et al. SYSTEM AND METHOD FOR DISCOVERING INTERNET PROTOCOL (IP) NETWORK ADDRESS AND PORT TRANSLATION BINDINGS. United States Patent Application Publication Pub . No.: US 2019 / 0089791 A1 Pub. Date: Mar. 21, 2019

[68] Jiang, T., Li, C., Wu, S., & Meng, S. (2019, July). Self-assembled micro-energy system based on block chain and IPV6. In AIP Conference Proceedings (Vol. 2122, No. 1, p. 020019). AIP Publishing.

[69] Hilal, R. (2019). Study of the Impact of Routing on the Performance of IPv4/IPv6 Transition Mechanisms. Smart Data and Computational Intelligence, 66, 43.

[70] Munadi, R., Sanjoyo, D. D., Perdana, D., & Adjie, F. (2019). Performance analysis of tunnel broker through open virtual private network. Telkomnika, 17(3).

[71] G. Lencse and Y. Kadobayashi, "Methodology for the identification of potential security issues of different IPv6 transition technologies: Threat analysis of DNS64 and stateful NAT64" Computers & Security (Elsevier), vol. 77, no. 1, pp. 397-411, August 1, 2018, DOI: 10.1016/j.cose.2018.04.012

[72] Akter, H., & Phillips, C. (2019). Tunnelling the internet. Australian Journal of Telecommunications and the Digital Economy, 7(1), 20.

[73] Sochor T., Sochorova H. (2019) Dynamic Routing Protocol Convergence in Simulated and Real IPv4 and IPv6 Networks. In: Silhavy R. (eds) Cybernetics and Automation Control Theory Methods in Intelligent Algorithms. CSOC 2019. Advances in Intelligent Systems and Computing, vol 986. Springer, Cham

[74] M. Koyuncu and H. AL-Fayyadh, "Comparison of scheduling algorithms for multimedia applications in IPv4 and IPv6," 2015 9th International Conference on Application of Information and Communication Technologies (AICT), Rostov on Don, 2015, pp. 418-422. doi: 10.1109/ICAICT.2015.7338592

[75] 44. Gulian, G. B. Distributed networks: modern technologies and design principles -Ed.: "MFP "synergy" MAGAZINE 2007-22 p.

[76] “IPv6 in Kazakhstan”, Tutorials point, [Online], Available: https:// https://ipv6-test.com/stats/country/KZ [Accessed By 03 February 2020]

Authors’ background

Your Name	Title*	Research Field	Personal E-mail
Gulzinat Ordabayeva	Phd student	Telecommunication & Networks Communication Protocols	gulzi200988@mail.ru
Mohamed Othman	full professor	Telecommunication & Networks	mothman@upm.edu.my
Bibinur Kirgizbayeva	full professor	Telecommunication & Networks	bibinur.kirgizbaeva@yandex.ru
Zhalgasbek Iztaev	associate professor	Information systems and modeling	Zhalgasbek71@mail.ru
Aigulim Bayegizova	Associate Professor	Radio engineering, electronics and telecommunications	baegiz_a@mail.ru