NEXT GENERATION INTERNET: IPv4 TO IPv6 TRANSITION MECHANISMS

Vasil Grozdanoski, Adrijan Božinovski
vasil.grozdanoskii@gmail.com, bozinovski@uacs.edu.mk
Faculty of computer science and information technology
University American College Skopje, Macedonia

Abstract— In the search of new technologies and methods for using the global network there is a need for using different technology approach rather than the current one. It is called IPv6.

In order to stop the usage of the old technology and to make a transition to the new one, it is necessary to take measures which will "smoothly" guide this process without any interruption of the work of the networks. Certainly this is not yet sufficiently developed and there it requires efforts to be done, but this paper elaborates the existing mechanisms that give big promises in this field. This paper focuses on the security issues which have a crucial role when it comes to internet protocols.

Furthermore, the paper makes a co mparison between IPv4 and IPv6 protocols, methods of transition from one protocol to another and the positive and negative outcomes. Finally, this paper contains a detailed description of the methodologies used to transit from the old to the new technology and their comparisons.

Keywords: Internet protocol. Internet, IPv4, IPv6, Unicast, host, subnet, broadcast

I. INTRODUCTION

Internet Protocol (IP) is a language and set of rules that computers use to "talk" to each other over the Internet [1]. The existing protocol that supports the Internet today is called Internet Protocol 4 (IPv4), which provides about 4 billion IP addresses, naturally limiting the number of devices that can assign unique and routable IP address on the Internet. The need for IPv6, which will allow the world a much greater number of IP addresses, is essential for the ongoing growth of the Internet and development of many new applications and expanding the mobile internet connections. Although the community of Information Technologies has been looking for shortcuts for solving this problem, it seems that IPv6 is a long- term solution.
Institutions should be prepared for the future networking of the Internet technology that will enable their networks to send and receive packets over IPv6 protocol. Translation of the protocols should be made with methodological awareness of its benefits and limitations [2].

II. INTERNET PROTOCOL VERSION 4 (IPV4)

IPv4 is the fourth generation of Internet protocols (IP) and first version that has been globally accepted. Along with IPv6 it is the base for interactive methods for working on the Internet. IPv4 is still the most developed protocol.
IPv4 is being introduced for the first time replacing RFC 760 protocol. IPv4 is protocol for using the packet-switched Link Layer networks, like Ethernet for example. It works as a model of "best delivery" where reliable delivery is not guaranteed, and doesn't provide reliable sequencing or avoid double delivery.
IPv4 does not own a mechanism for error control or flow control. However, it discards data which is found as damaged with the method of checking the sum (checksum), which is located in the datagram header.
Including these aspects which are used for data integrity, they are addressed by higher level of protocol, such as Transmission Control Protocol (TCP).
IPv4 uses 32bit addressing which enables 4,294,967,296 unique addresses. IPv4 has 4 different types of classes: A, B, C and D [3].

A. Architecture for IP network addressing

At the beginning, IP addresses where divided into two parts: network identifier that has the highest order in the network address and host identifier that uses the other parameters of the address. This mechanism generated most of 256 ne tworks, which was inadequate. To overcome this limit, the highest order in the network address was redefined to make a set of classes of networks in a system that was later called classfull. This system had 5 classes A, B, C, D and E.

A, B and C classes had different bit length for the new network identification. The rest of the address was used as before to define "host" in a network, which meant that every network class had a different capacity of address host. Class D was intended for multicast addressing and class E was intended for future applications.

B. *Creating subnets*

Creating subnets is a set of tehniques that can be used for efficiant deviding the address space of unicast address prefix for alocationg the network addresses in oganizational networks. The fixed position of unicast address prefix includes bits that have defined value.

The variable part of unicast address prefix includes parts outside of the prefix with lengths which are set to 0.

Creating subnets is used for the variable part of unicast address prefix to create address of prefixes that are more effective (to exclude as less as possible addresses) for assigning subnets in an organizational network.

Creating subnets for IPv4 originally was defined to improve the use of host bits for class A and class B of IPv4 public address prefixes.

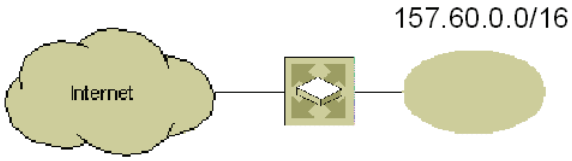

Figure 1. Network 157.60.0.0/16 before creating subnets [4]

At the subnet, using the B class address can support up to 65 534 nodes, which is too much to have on same subnet.

With simple creation of subnets, 157.60.0.0/16 subnet can be defined with using the first 8 bits from the host. If subnet 157.60.0.0/16 is created, like shown in *figure 1,* the subnet will be created with own prefixes (157.60.1.0/24, 157.60.2.0/24, 157.60.3.0/24) with 254 hosts on each subnet. The router will became "aware" of the special subnet addresses and it will route IPv4 packets to the appropriate subnet.

III. NEED FOR A NEW GENERATION OF INTERNET

As mentioned above, IPv4 brings fixed number of IP addresses, so it takes the inability to support new machines connected to Internet, unlike IPv6, which brings almost unlimited number of IP addresses and can support new computer systems.

The lack of IPv4 address space also reduces announcement of new applications, new and innovative services, that can work at the home and business networks.

Without a sufficient number of address space, applications are forced to work in a much more complex environment, with mechanisms that provide local addressing, like IP address conversion, pooling and techniques for temporary allocation.

Current Internet cannot support a solution for large number of problems, including: national security, economic competiveness and social goals.

Maybe by defining the features of the new generation of Internet the speed will have the top priority. This generation of Internet will primary begin to adjust towards increasing the traffic and high bandwidth in order to meet the demands of higher level of required Internet speed. The next generation of Internet will sort the problem with busy dial- up lines and poor quality of audio and video transmission [5].

IPv6 is the next generation of Internet which uses the IP addresses and will be widely accepted as an Internet protocol. Compared with IPv4 which enables use of 4, 294,967,296 unique addresses, IPv6, which uses 128bit system, will enable 10^36 or, more precisely 34, 000, 000, 000, 000, 000, 000, 000, 000, 000, 000, 000, 000 IP addresses. This is more than the number of stars that mankind knows. It is announced that IPv6 will be massively used from year 2025, and till then it will have to solve some details that may occur as negative [6].

An IP address example:

207. 142. 131. 235. 207. 142. 131. 235. 207. 142. 131. 235. 207. 142. 131. 235.

IV. WHY IPV6?

One of the reasons why IPv6 should be used in future is the earth population and distribution of the Internet world wide. Also, in the future cars will be driven by navigation that will use IP addresses, so we will need more unique IP addresses then we have at this moment.

A. *IPv6 address format*

In order to adjust the almost unlimited and diversity of IP addresses, IPv6 uses 128bit length.

IPv6 has three types of addresses defined:

- **Unicast address** defining one host
- **Anycast address** is the address which is dedicated on more than one interface and mostly belongs to different IPv6 nodes, similar to set of routers that belong to one Internet Service Provider (ISP). A packet sent to anycast address is delivered to one of the routers identified from that address, mostly the closest one which is defined from the routing protocol.
- **Multicast address** also identifies a set of hosts. Packets sent to multicast address are delivered to all hosts in the group.

It should be noted that there is no broadcast address in IPv6 unlike IPv4, because the function is determined by the multicast address.

IPv4 are written in dotted decimal notation, where the decimal value is separated by dots (.). In IPv6, the notation is represented in hexadecimal value with 8 16bit blocks of

addresses separated by (:), like FF04:19:5:ABD4:187:2C:754:2B1 for example.
It should be noticed that the lead zeroes do not have to be written and that every field must have some value.
The alternative, hybrid address format is defined to make more convincing for representing the IPv4 address in IPv6 environment.

In the next chart, the first 96 address bits (6 groups of 16) are presented in regular IPv6 format, and the next 32 address bits are presented in IPv4 dotted notation.
Example 0:0:0:0:0:0:199.182.20.17 (or ::199.182.20.17).

B. ICMPv6

When the data travels from the sender to the receiver, for some reason there is a chance it does not reach the receiver. ICMPv6 always sends a report for the status of the sent packet to (ICMP). The Internet Control Message Protocol generates a message for the status of the link that's being sent. Messages from the ICMPv6 are saved in IPv6 datagram with Next Header field with a value of 58.

The error messages of ICMPv6 are:

- Destination Unreachable- sent when one packet cannot be delivered to its destination from various congestion reasons
- Packet Too Big- sent from router when packet cannot be delivered, because the packet is larger than *maximum transmission unit* (*MTU*)
- Parameter Problem- sent by the node when a problem will occur in header field of the packet, which results with inability to process.

Table 1. Scheme representation of IPv4 and IPv6 address bits [7]

ALLOCATION	Prefix (binary)	Fraction of Address Space
Reserved	0000 0000	1/256
Unassigned	0000 0001	1/256
Reserved for NSAP Allocation	0000 001	1/128
Reserved for IPX Allocation	0000 010	1/128
Unassigned	0000 011	1/128
Unassigned	0000 1	1/32
Unassigned	0001	1/16
Unassigned	001	1/8
Provider-Based Unicast Address	010	1/8
Unassigned	011	1/8
Reserved for Geographic-Based Unicast Addresses	100	1/8
Unassigned	101	1/8
Unassigned	110	1/8
Unassigned	1110	1/16
Unassigned	1111 0	1/32
Unassigned	1111 10	1/64
Unassigned	1111 110	1/128
Unassigned	1111 1110 0	1/512
Link Local Use Addresses	1111 1110 10	1/1024
Site Local Use Addresses	1111 1110 11	1/1024
Multicast Addresses	1111 1111	1/256

C. IPv6 security

The use of Internet is rapidly growing, so there is a risk for large dataflow. Security here is at first place. Although today's TCP/TP applications have their protection mechanisms, many would say that the security should be implemented at the lowest protocol level.

IPv4 has several protective mechanisms, but not on the low level protocols. IPv6 has built two security schemes on the basic protocols:

1. The first mechanism is IP Authentication Header (RFC 1826), extending the header, which can provide integrity and authentication for IP packets. Although a lot different techniques for authentication will be supported, using the encrypted message (Message Digest 5 MD5) will be required to provide interoperability. Using this option can eliminate high number of network attacks, like IP address spoofing. This will be also an important supplement to overcome some security weaknesses of IP routing. IPv4 does not provide host authentication. It just allows the host address in the IP datagram. Putting information for host authentication in the Internet layer in IPv6 allows essential protection on high level protocol.

2. The second mechanism is e IP Encapsulating Security Payload ESP, extended header that provides integrity and security for the IP packets. Although the definition for ESP is that it is not dependent from an algorithm, Data Encryption Standard (DES-CBC) is described as standard schema for encryption providing interoperability, ESP mechanism can be used to encrypt whole IP packet (*tunnel-mode ESP*) or just the highest level of (*transport-mode ESP*).

These options will add to the security of the IP traffic significantly reducing security "effort". Authentication of end-to-end basis during the session setup will provide secure communication even without presence of routers with firewalls [8].

V. IPV4 TO IPV6 TRANSITION MECHANISM

The transition between the IPv4 Internet today and the IPv6 Internet of the future will be a long process during both protocols coexists. Figure 1 shows the transition phases. A mechanism for ensuring smooth, stepwise and independent changeover to IPv6 services is required. Such a mechanism must help the seamless coexistence of IPv4 and IPv6 nodes during the transition period. Internet Engineering Task Force (IETF) has created a group to facilitate the smooth transition from IPv4 to IPv6 services. They're divided into three groups:

- dual stack
- tunneling
- header translation

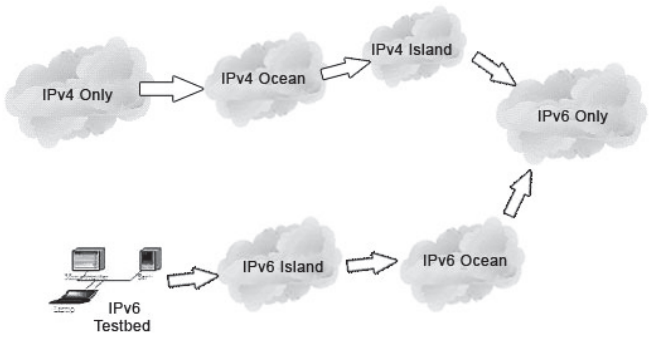

Figure 2. Stages of transition [9]

A. IPv4/IPv6 dual stack mechanism

As the word means, dual-stack mechanisms include two protocol stacks that operate in parallel and allow network nodes to communicate either via IPv4 or IPv6. They can be implemented in both end system and network node. In end systems, they enable both IPv4 and IPv6 applications to operate at the same time. The Dual-stack capabilities of network nodes support the transport of both IPv4 and IPv6 packets.

Table 2. Dual-stack transition mechanism [10]

IPv4 applications	IPv6 applications
Sockets API	
UDP/TCPv4	UDP/TCPv6
IPv4	IPv6
L2	
L1	

IPv4 applications use IPv4 stack and IPv6 applications use IPv6 stack.

Flow decisions are based on the version field of IP header for receiving, and on the destination address type for sending. The types of addresses are usually derived from DNS lookups; the appropriate stack is selected in response to the types of DNS records returned. Many off-the-shelf commercial operating systems already have dual IP protocol stacks.
Hence, the dual-stack mechanism is the most extensively employed transition solution. However, dual stack mechanisms enable only similar network nodes to communicate with each other (IPv6-IPv6 and IPv4-IPv4). Much more works are required to create a complete solution that supports IPv6-IPv4 and IPv4-IPv6 communications.

B. IPv4/IPv6 tunneling mechanisms

Tunneling, from the perspective of transitioning, enables incompatible networks to be bridged, and is usually applied in a point-to-point or sequential manner. Three mechanisms of tunneling are presented:

- IPv6 over IPv4,
- IPv6 to IPv4 automatic tunneling,
- Tunnel Broker.

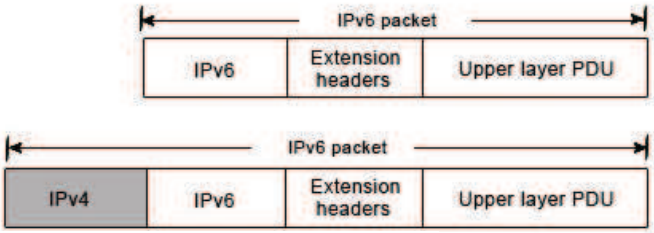

Figure 3. Address identifier of layer [11]

1. IPv6 over IPv4

This protocol embeds an IPv4 address in an IPv6 address link layer identifier part and defines Neighbor Discovery (ND) over IPv4 using organization-local multicast. An IPv4 domain is a fully interconnected set of IPv4 subnets, within the scope of a single local multicast, in which at least two IPv6 nodes are present. The IPv6 over IPv4 tunneling setup provides a solution for IPv6 nodes that are scattered throughout the base.

2. IPv6 to IPv4 Automatic Tunneling Mechanism

Automatic tunneling refers to a tunnel configuration that does not need direct management. An automatic IPv6 to IPv4 tunnel enables an isolated IPv6 domain to be connected over an IPv4 network and then to a remote IPv6 networks. Such a tunnel treats the IPv4 infrastructure as a virtual non-broadcast link, so the IPv4 address embedded in the IPv6 address is used to find the other end of the tunnel.

The embedded IPv4 address can easily be extracted and the whole IPv6 packet delivered over the IPv4 network, encapsulated in an IPv4 packet.

Figure 4 shows the structure of the 6to4 address format. The value of the prefix field (FP) is 0x001, which identifies the global unicast address. The Top-Level Aggregation identifier field (TLA) is assigned by the IANA for the IPv6 to IPv4 mechanism. Hence, the IPv6 address prefix is 2002::/16 and the 32 bits after 2002::/16 represent the IPv4 address of the gateway machine of the network in question. The 6to4 mechanism is the most widely extensively used automatic tunneling technique. It includes a mechanism for assigning an IPv6 address prefix to a network node with a global IPv4 address.

3. IPv6 Tunnel Broker

The IPv6 Tunnel Broker provides an automatic configuration service for IPv6 over IPv4 tunnels to users connected to the IPv4 Internet. IPv4 connectivity between the user and the service provider is required. The service operates as follows:

1. The user contacts Tunnel Broker and performs the registration procedure.
2. The user contacts Tunnel Broker again for authentication and providing configuration information (IP address, operating system, IPv6 support software, etc.).
3. Tunnel Broker configures the network side end-point, the DNS server and the user terminal.
4. The tunnel is active and the user is connected to IPv6 networks.

C. IPv4/IPv6 header translation

The basic function of translation in IPv4/IPv6 transition is to translate IP packets. Several translation mechanisms are based on the SIIT (Stateless IP/ICMP Translation algorithm) algorithm. The SIIT algorithm is used as a basis of the BIS (Bump In the Stack) and NAT-PT (Network Address Translation-Protocol Translation) mechanisms.

1. Bump-In-the-Stack mechanism

BIS mechanism includes a TCP/IPv4 protocol module and a translator module, which consists of three bump components and is layered above an IPv6 module. Packets from IPv4 applications flow into the TCP/IPv4 protocol module. The identified packets are translated into IPv6 packets and then forwarded to the IPv6 protocol module. The three bump components are:

- the extension name resolver, which examines DNS lookups to determine whether the peer node is IPv6-only;
- the address mapper, which allocates a t emporary IPv4 address to the IPv6 peer and caches the address mapping;
- the translator, which translates packets between IPv4 and IPv6 protocol.

2. Network Address Translation-Protocol Translator

The Network Address Translation – Protocol Translation (NAT- PT) mechanism is a statefull IPv4/IPv6 translator. NAT-PT nodes are at the boundary between IPv6 and IPv4 networks. Each node maintains a pool of globally routable IPv4 addresses, which are dynamically assigned to IPv6 nodes when sessions are initiated across the IPv6/IPv4

boundary. This mechanism allows native IPv6 nodes and applications to communicate with native IPv4 nodes and applications, and vice versa.

The NAT-PT mechanism is an interoperability solution that needs no modification or extra software, such as dual stacks, to be installed on any of the end user nodes, either the IPv4 or the IPv6 network. This mechanism implements the required interoperability functions within the core network, making interoperability between nodes easier to manage and faster to manifest [12].

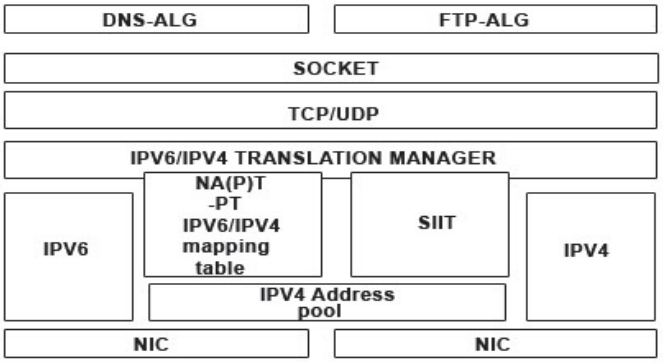

Figure 4. NAT-PT protocol architecture [13]

VI. CONCLUSION

IPv4 is „extinction kind". It's like the license plates of the cars- there are a lot of combinations from numbers and letters that can be made, so when planning it seems that they will meet the needs of all users. Over time, the traffic increases and the people are buying more cars. What happens to the old cars? Some of them are no longer in use, but they still hold their plates, so there is a need to provide new plates to the new cars.

Perhaps the most "creditable" for "traffic congestion" are the VPN networks which certainly must have static IP addresses where secure communication takes place. This method is mostly used by the banks and other institutions that have a need of this kind of data transfer.

However, the increased use of the technology cannot meet the 4,294,967,296 IPv4 addresses in the "www global village", so IPv6 takes the stage with 34,000,000,000,000,000,000,000,000,000,000,000,000 IP addresses.

Maybe this seems like a lot, but in a free estimate for the next 30- 50 years engineers will be dealing with full hands of work. Whether the reason for lack of IP addresses which will occur or by the chaos that will be made, it remains to be seen.

REFERENCES

[1] D.Shalini Punithavathani Registrar, K.Sankaranarayanan, IPv4/IPv6 Transition Mechanisms, Anna University Tirunelveli, India, 2009

[2] Meenakshi Gupta, Lecturer, Maharaja, IPV 4 vs. IPV 6 – The Next Generation Internet, Agarsen Institute of Technology Affiliated to GGSIPU, February 25 – 26, 2010

[3] Ipv6 Return On Investment (R.O.I) Analysis Framework At A Generic Level, And First Conclusions, ERIM REPORT SERIES RESEARCH IN MANAGEMENT, September 2002

[4] Joe Davies, microsoft technet, Chapter 4 – Subnetting, December 14, 2004, http://technet.microsoft.com/en-us/library/Bb726997.subtn402_big(l=en-us).gif, last accessed on 23.01.2012

[5] West Lafayette, Sherali Zeadally, Evaluating IPv4 to IPv6,
Purdue University 1398 Computer Science Building, Detroit USA, 2008

[6] Emdad, What is an Internet Protocol Version 4 (IPv4) address?, 2011, http://emdadblog.blogspot.com/2010/07/what-is-internet-protocol-version-4.html, last accessed on 03.02.2012

[7] Joel Snyder, What is IPv6?, http://www.opus1.com/ipv6/whatisipv6.html, 1997, last accessed on 03.02.2012

[8] European IPv6 Task Force & Steering Committee IPv6 Forum, IPv6 Summit, IPv6 is an innovation opportunity, Education & Promotion WG Co-chair Consulinela, Madrid 2005

[9] Neil Gershenfeld, Internetworking Technology Overview, June 1999, http://fab.cba.mit.edu/classes/MIT/961.04/people/neil/ip.pdf, last accessed on 03.02.2012

[10] Geoff Huston, Is the Transition to IPv6 a "Market Failure?", September 2009, http://www.potaroo.net/ispcol/2009-09/fig2.jpg, last accessed on 18.01.2012