ANALYSIS OF IPV4 TRANSITION METHODS FOR IPV6: FEATURES, ADVANTAGES AND DISADVANTAGES

ANÁLISE DOS MÉTODOS DE TRANSIÇÃO DO IPV4 PARA O IPV6: CARACTERÍSTICAS, VANTAGENS E DESVANTAGENS

Leonardo Donizetti Bueno*
Adinovam Henriques de Macedo Pimenta**

ABSTRACT

The Internet has seen exponential growth in recent decades, and Internet Protocol Version 4 (IPv4), with 32 bits, was the leading player in Internet development and expansion around the world. However, the increase in the demand for hosts caused a depletion of the IPv4 addresses, thus demanding the need for a more effective protocol in this sense. Thus, to solve the problem of address exhaustion, the Internet Protocol Version 6 (IPv6) was developed, whose addresses are formed by 4 times more bits than IPv4, totaling 128 bits. With the objective of replacing IPv4 in a gradual way so that when IPv4 was discontinued every network was already able to the new protocol, the transition techniques came to be seen as fundamental tools for this process, thus contributing to implementation of IPv6 occurs more broadly. Based on this assumption, this work has as main objective to describe the characteristics, advantages and disadvantages of the main transition techniques from IPv4 to IPv6, comparing each of them to a better understanding and understanding of the process. To meet this objective, we sought to describe the general aspects of the IPV4 protocol; understand the difference between IPv4 and IPv6; addressing aspects of the IPv4 and IPv6 header; and describe the most used transition techniques, such as tunneling, translation and double stack, listing the main differences between them.

Keywords: Transition from IPv4 to IPv6. Internet protocol. Double Stack. Translation. Tunneling.

RESUMO

A internet viveu um crescimento exponencial nas últimas décadas, e o protocolo de rede *Internet Protocol Versão* 4 (IPv4), com 32 bits, foi o principal protagonista do desenvolvimento e expansão da internet por todo o mundo. No entanto, o aumento da demanda por *hosts* ocasionou o esgotamento dos endereços IPv4, demandando, dessa forma, a necessidade de um protocolo mais efetivo nesse sentido. Assim sendo, para sanar o problema de esgotamento de endereços, foi desenvolvido o *Internet Protocol Versão* 6 (IPv6), cujos endereços são formados com uma representatividade por 4 vezes maior que o IPv4, totalizando 128 bits. Com o objetivo de substituir o IPv4 de forma gradativa, a fim de que quando houvesse a descontinuação do IPv4 toda rede já estivesse

* Graduation in Computer Science at the Faculdade de Tecnologia, Ciências e Educação (FATECE). leobueno42@gmail.com
** Lecturer in Computer Science at the Faculdade de Tecnologia, Ciências e Educação (FATECE). adinovam@icmc.usp.br

apta para o novo protocolo, as técnicas de transição passaram a serem vistas como ferramentas fundamentais para esse processo, contribuindo, assim, para que a implantação do IPv6 ocorra de forma mais ampla. Partindo desse pressuposto, esse trabalho tem como objetivo principal descrever as características, vantagens e desvantagens das principais técnicas de transição do IPv4 para o IPv6, comparando cada uma delas para um melhor entendimento e compreensão do processo. Para atender esse objetivo, buscou-se descrever os aspectos gerais do protocolo IPv4; compreender a diferença entre o IPv4 e o IPv6; abordar os aspectos do cabeçalho desses dois protocolos; e descrever as técnicas de transição mais utilizadas, como o tunelamento, tradução e pilha dupla, elencando as principais diferenças existentes entre elas.

Palavras-chave: Transição do IPv4 para o IPv6. Protocolo de Internet. Pilha Dupla. Tradução. Tunelamento.

Introduction

In general, the Internet can be understood as a network that interconnects several other computer networks around the world. For this process to occur, it makes use of the so-called Internet Protocol (IP), which is responsible for allowing computers that are part of the network to use a single address to communicate. In this sense, the IP protocol commonly used is IPv4 (Internet Protocol version 4). Each IPv4 address consists of 32 bits, thus totaling about 4 billion addresses. However, as technology progresses, IPv4 addresses have begun to run out, with the need to update the protocol to meet the new demands.

In order to extend the addressing service, the IPv6 (Internet Protocol version 6) protocol has been developed, which allows addresses to have a larger capacity, 128 bits, and consequently generate a much larger number of IP addresses. In this way, the IPv6 protocol came to be seen as a tool of extreme relevance to meet the demands of IP addressing, but with some doubts about how the transition from IPv4 to IPv6 should occur, and what would be the best techniques for this process.

Based on this assumption, this work is justified by the need to understand the general aspects of IPv6 and what are the existing transition techniques in order to promote a greater understanding of the advantages and disadvantages of each of them. In addition, with the accomplishment of this work, it is sought to know better the characteristics of the IPv6 protocol, as well as to understand the difficulties encountered in the transition process, which justifies the importance of understanding the characteristics of the techniques directed to the use of this new protocol .

Taking into account that IPv6 expands the amount of addressing, in addition to adding new security and performance features so that hardware or software manufacturers can choose to upgrade their equipment at different times without interrupting the flow of data on the internet, unlike of the IPv4 protocol, this study has as guiding question the following question: What are the most used transition techniques from IPv4 to IPv6?

As a main objective, this work aims to describe the characteristics of the main transition techniques from IPv4 to IPv6, each one of them for a better understanding and understanding of the process of migration to version 6. In order to meet this objective, an attempt was made to describe the general aspects of the IPv4 and IPv6 protocols, in order to understand the difference between them; identify the features of IPv6; and describe the transition techniques from IPv4 to IPv6, such as tunneling, translation and double stack, enumerating the main differences between them.

This work uses as a bibliographical research methodology, and is based on the qualitative approach, with an analysis of elements that permeate the transition theme from IPv4 to IPv6, as well as the importance that the transition techniques have for this process, form, purpose and problem mentioned above. In order to carry out this study, several contributions were made by scholars of the subject published in books and scientific articles, disregarding the phenomena that did not have scientific background and relation with the proposed objective.

1 Theoretical Reference

The Internet was developed from grants from Defense Advanced Research (DARPA) to create a non-centralized, fault-tolerant network. According to Aparecido (2012), when conceived in the late 1960s, the Internet had only four network nodes and, by the end of the 1980s, it had the current structure based on the IP protocol.

At the time of its development, the internet did not require mobility and security for personal use. However, in the beginning of the 1990s, the popularization of the internet and all the convenience provided by the emergence of web servers and browsers, search engines, e-commerce, internet banking and other online services, as Brito (2013, p. 22) points out "Impacted on the unbridled growth of the network with an increasing number of users", thus requiring a relevant update on the IP network protocol, as will be pointed out below.

1.1 General Aspects of IPv4 and IPv6 Protocols

Evolution, inherent in the human species, allowed the emergence of numerous tools to facilitate the living and communication of the human being, as well as the development of society. In this way, innumerable resources, including technology and the internet, have emerged as tools aimed at the growth of cities, among others, facilitating all communication processes between them.

Based on this assumption, Santos (2013) points out that the worldwide computer network in the last decades, through Internet access, has grown too users, causing a greater concern about the exhaustion of IP protocol addresses, which represent the identity of each of these users worldwide in the network.

In relation to the protocols, according to the data of Filippetti (2011), what usually is widely used is the version 4, denominated of IPv4, that has a capacity of 32 bits for the addresses in the Internet. In addition, according to the author, this version is divided into classes, network numbers and host numbers.

Complementing this statement, Silveira (2012) says that the aspects that were not foreseen in the creation of IPv4 were the possibility of network growth, as well as the exhaustion of IP addresses. In this sense, numerous problems began to arise regarding the security of the data that was transmitted, as well as in the delivery of certain types of data packets.

The IPv4 protocol is the technological base of the internet and according to Aparecido (2012, p. 48) "works with addresses of 4 bytes. It was released in 1979 on a date when it was not possible to predict how much the internet would grow because at the time the 4 billion possible addresses were considered more than sufficient.

Taking into account that the Internet was used not only in personal computers, but also in other types of technological instruments, such as mobile phones, tablets and smartphones, the network started to have a larger number of users, exhausting the addresses of IP.

To solve this adversity, Cordeiro (2014) points out that the solution found was to upgrade version 4 of the protocol to a larger version that could satisfy the real growth conditions of the internet. In this sense, the IPv6 protocol was presented, which was specified by RFC 2460 in December 1998.

Also according to Cordeiro (2014), IPV6, in relation to IPv4, presents a number of significant changes, such as greater addressing capacity, simplification in the format of the header (which will be pointed out in the course of this study), support to include extension headers, data stream identification, and also support for user authentication and privacy.

To Comer (2005), IPv6 allows a more effective revision of the datagram format, something that IPv4 did not do. In addition, it has 128 separate bits in networks and hosts, which meets demand beyond what is necessary for the worldwide network, since it offers billions of addresses.

It is important to describe that each address consists of a prefix called Net-Id, which identifies the network, and also a suffix, called Host-Id, that allows the identification of the station interface in the particular network (COLCHER et al. 2005).

Unlike IPv4, version 6 does not use palliative solutions techniques, such as Network Address Translator (NAT) and Classless Interdomain Routing (CIDR), which are techniques for optimizing IPv4 addresses. According to Colcher et al. (2005), the non-use of these techniques by version 6 avoids wasting addresses that could be used by more users, since they got stuck in those programs.

It is noticed that due to the extensive addressability of version 6, the constant need for protocol improvement features becomes unnecessary, which results in a significant improvement in packet routing, given that the router no longer needs to process these parallel features.

Another important point highlighted by Machado (2015) in relation to IPV6 is that unlike version 4, the use of addresses is measured against the demand for allocation of assignments /48 to end users, and no longer to the number of addresses that were made available to them. In this context, for the local networks, the recommended size becomes the /64 with stateless addressing.

As previously pointed out, version 6 of the protocol has a 128-bit field for its addresses, thus reaching a size sufficiently capable for users of future generations for a significantly longer time. In this context, Heidrich (2011) says that the denotation of IPv6 is hexadecimal with two points, providing a better and more compact view than the decimal in version 4.

As in IPv4, the basic IPv6 addresses are defined, as follows: unicast, anycast and multicast. The first, unicast, refers to the type of address that identifies a single host, and has a packet delivered by the shortest path. The anycast has the destination identified by a set of hosts and the packet is delivered to one of them. Finally, multicast also represents a set of hosts, but the packet is not forwarded to only one of them, but to all the interfaces of the same address (SANTOS et al., 2010).

Being common in IPv4, version 6 does not present a broadcast address, that is, sending packets to all who use the same domain. According to Comer (2005), this function was added to the multicast.

As Internet use, for the most part, comes from the IPv4 protocol, it is important to emphasize that the transition to the new version must be done in a gradual and appropriate way to the demands. According to Santos (2013), the exchange can not be done on all sites and servers suddenly, because the damages would be severe. Thus, transition techniques were developed that serve to realize the exchange without causing adversity for the users, mainly corporations that use the network in a continuous way.

The IPv6 protocol is intentionally designed to minimize the impact on layered protocols, avoiding the random addition of new features. The potential commercial benefits resulting from IPv6 include lower network administration costs, protecting company assets through a unified security model, protection by gradual transition, and deployment of new applications (FILIPPETTI, 2011).

Table 1 - Comparison between IPv4 and IPv6

IPv4	**IPv6**
32-bit address	128-bit address
Optional IPSec support	Required IPSec Support
No reference to QoS (Quality of Service)	It introduces QoS capability using the Flow Label field
Fragmentation process performed by the router	Fragmentation is no longer performed by the routers and is then processed by the sending hosts
The header includes the option fields	All the option fields have been changed into the extension header field

Source: Adapted from Cisco, 2013

According to the data described in Table 1, it is observed that there is a considerable difference between the protocols version 4 and 6 in their technical aspects, which justifies the necessity of its transition in order to allow a sufficient number of addressing to serve the users network.

In addition, Comer (2005) highlights that version 6 of the protocol "introduced the concept of extension header (optional). These headers can be created for the purpose of providing extra information as long as they are efficiently encoded". “IPv6 changes the format of the datagram relative to IPv4. It presents a simplified base header that uses only essential fields, and other optional fields can also be added to the datagram through extension headers" (COMER, 2005, p. 540).

As such, the next section will address the main aspects of IPv6 functionality, which contributes to a better understanding of the importance of transitioning from version 4 to version 6 of the network protocol.

1.2 Features of Internet Protocol version 6 (IPv6)

Regarding the transition from IPv4 to IPv6, it is extremely important to understand the features of this new protocol, since they are fundamental for the process to occur in a uniform way and obtain positive results. In this context, Cisco (2013) points out that for IPv6 to be implemented through the use of transition techniques it is necessary to use an auxiliary protocol, called Internet Control Message Protocol Version 6 (ICMPv6).

ICMPv6 uses messages as a means of exchanging information in the application of the desired tool, informing the network types, diagnosing the network and reporting cases of errors that may occur during processing. According to Heidrich (2011), for ICMPv6 to correctly address messages, it is important that it be deployed to all nodes of the network, since it is not compatible with version 4.

Another important factor is that the messages obtained by ICMPv6 precede the basic header of version 6 and also the extension headers, as shown in Chart 1.

Chart 1 – ICMPv6 Header Position

Basic IPv6 Header	Extension Header 1-N	ICMPv6 Header

According to Cisco (2013), for IPv6 to function correctly, the ICMPv6 messaging protocol is essential because it manages numerous functions, such as multicast address groups, address resolution of the lower layer, messages for the Discovery function Neighborhood, Maximum Transmit Unit (MTU) discovery, and stateless address types.

In addition to these factors, ICMPv6 is divided into two types of message groups: error messages and informational messages. According to Santos et. al. (2010), these message groups are described according to the data indicated in Tables 2 and 3.

On the Discovery of Neighborhood feature, it refers to the communication task between nodes in a version 6 network, which resembles version 4 because it used the

ARP protocol. According to Cisco (2013), the IPV6 has as complement in this process the use of additional methods in its structure, allowing a greater reach of the results.

For Santos et al. (2010), the Neighborhood Discovery has many relevant characteristics, such as the determination of the address in the layer of the OSI model, meeting of directly connected routers, besides access to them, and determination of network configurations and addresses.

The stateless addressing function refers, according to Silveira (2012) to the task of assigning the IP address automatically to the host, a process that is called Stateless Address Autoconfiguration. Bypassing the process of manually configuring the address server, this IPv6 feature uses the 64-bit Extended Unique Identifier (EUI-64) standard to configure the IPv6 address on the fixed destination networks.

Table 2 - ICMPv6 Error Messages

TYPE	NAME	DESCRIPTION
1	*Destination Unreachable*	When the packet send destination is not reachable or has transmission failure.
2	*Packet Too Big*	When the packet exceeds the MTU.
3	*Time Exceeded*	Exceeded the reassembly time or the maximum limit for the jumps in the links.
4	*Parameter Problem*	Header issues.

Source: Adapted from Santos et al., 2010.

Table 3 - ICMPv6 Information Messages

TYPE	NAME	DESCRIPTION
128	*Echo Request*	*Ping* command.
129	*Echo Reply*	
130	*Multicast Listener Query*	Multicast Group Management
131	*Multicast Listener Report*	
132	*Multicast Listener Done*	
133	*Router Solicitation (RS)*	Neighborhood Discovery
134	*Router Advertisement (RA)*	
135	*Neighbor Solicitation (NS)*	
136	*Neighbor Advertisement (NA)*	

137	*Redirect Message*	
141	*Inverse ND Solicitation Message*	Neighborhood Discovery Extension Messages
142	*Inverse ND Advertisement Message*	
151	*Multicast Router Advertisement*	Discovery of neighboring routers
152	*Multicast Router Solicitacion*	
153	*Multicast Router Termination*	

Source: Adapted from Santos et. al., 2010.

In view of the foregoing, understanding these main features allows the transition techniques from version 4 to version 6 to occur in a concise manner, allowing the adoption of IPv6 does not cause major problems and, consequently, meets the purposes for which this new version was created.

2 Main Transition Techniques from IPv4 to IPv6

As previously described, due to the numerous changes in the IP protocol coming from version 6, it becomes incompatible with IPv4, previous version, demanding an effective migration process. According to Silveira (2012), during the migration process, the IPv4 and IPv6 protocols must coexist, allowing the change to occur gradually.

According to Cisco (2013), there are about three most commonly used types of transition methods: tunneling, NAT64 / DNS64 translation, and dual stack, in which they are classified according to their functionality. Therefore, each of these techniques will be described below, listing its main characteristics and functioning.

2.1 Dual Stack

In general, this technique can be understood as the coexistence of IPv4 and version 6 in the same equipment, both being active simultaneously. According to Felippetti (2011), this migration technique for IPv6 is seen as the default and should be used whenever possible on the Internet.

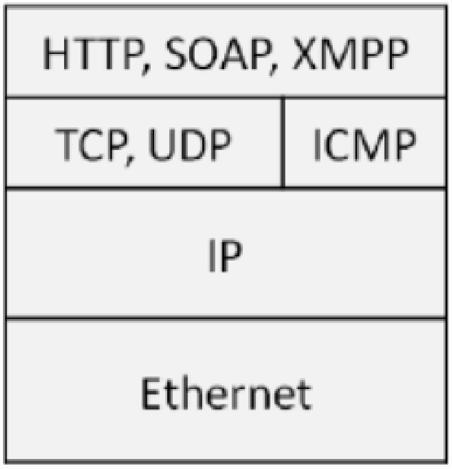
According to Santos (2013), in the transition process, it is extremely important to maintain compatibility with IPv4 while version 6 is being deployed to streamline the internet transition. In this sense, the author states that it is necessary to take into account the implementation of the dual stack technique, since it allows the gradual migration with the two protocols in operation in the network.

Based on this assumption, the dual stack technique is formed by the coexistence of version 4 and 6 in the same equipment, allowing it to be able to send and receive the two types of packets. In this sense, Moreiras (2012) states that a Double Stack node behaves as an IPv6 node within the communication with another IPV6 node, and the same process occurs in the case of the IPv4 node.

In order for this communication to be possible, that is, for it to occur with the use of both protocols, it is important that mechanisms be used to configure the addresses, allowing each device to have both an IPv4 and an IPv6 address (MOREIRAS, 2012).

In the dual stack, IPv6 / IPv4 nodes use IPv4 mechanisms to acquire their IPv4 addresses, as in the case of DHCP, and IPv6 mechanisms to acquire IPv6 addresses, such as stateless address autoconfiguration. Thus, the operation of this technique can be observed according to the data of Figure 1.

Figure 1 - Dual Stack Operation



Source: Adapted from IPv6.br (2012)

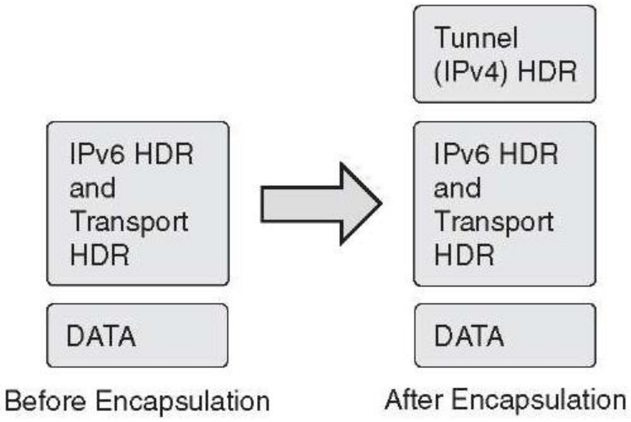
As pointed out in Figure 1, it can be seen that the Dual Stack technique allows a version 6 deployment to occur gradually, through the configuration of small sections of the network environment at a time. In addition, according to Moreiras (2012), if the IPv4 protocol is no longer used in the future, it is enough to disable the stack that refers to the version within each node.

2.2 Tunneling

The IPv6-over-IPv4 tunneling, according to Moreiras (2012), refers to the establishment of point-to-point tunnels by means of a process of encapsulating the existing packages in version 6 within the headings of version 4, which allows a load on the existing infrastructure in IPv4 routing, as shown in Figure 2.

According to Silveira (2012), the process of encapsulating is called 6in4 or IPv6-in-IPv4, and does not contemplate the possibility of creating a greater coexistence between version 4 and 6. According to the author, unlike the double stack, the tunneling technique allows communication between the IPv6 islands through the version 4 networks because it encapsulates the datagrams of version 6 in the previous version. However, by means of tunneling it is not possible for the version 6 islands to communicate with the version 4 networks, thus preventing the development of a coexistence scenario between the networks in the migration process.

Figure2 – Tunneling *IPv6-over-IPv4*.



Source: WHAT-WHEN-HOW (2018)

Even with these observations, tunneling can be considered the most used method in the initial phase of the migration to IPv6, since it transmits the packages of version 6 in IPv4 networks, without the need to make changes in the routing mechanisms. In this context, Moreiras (2012) points out that by encapsulating the contents of the IPv6 packet in an IPv4 packet, where the tunnel input node creates an IPv4 header with the encapsulated IPv6 packet and transmits it over the IPv4 network.

Although there are these observations, it is emphasized that the Dual Stack technique allows the coexistence of both versions in the migration process, a factor that allows a greater capacity of implantation of the new protocol version, without any kind of use impairment version 4.

Regarding tunneling, this technique has the following classification (CISCO, 2013):

- Router-to-Router: IPv6 / IPv4 routers connected via IPv4 network that can exchange packets of version 6 with each other;
- Host-to-Router: IPv6 / IPv4 hosts send IPv6 packets to an intermediate IPv6 / IPv4 router via the IPv4 network;
- Router-to-Host: IPv6 / IPv4 routers send IPv6 packets to the final IPv6 / IPv4 destination;
- Host-to-Host: IPv6 / IPv4 hosts, connected via IPv4 network, exchange IPv6 packets with each other.

In addition to this classification, tunneling is characterized by numerous types, such as Tunnel Broker (allows iPV6 / IPv4 hosts isolated on a version 4 network to access the version 6 network); 6to4 (allows the communication between hosts of version 6 by the infrastructure of version 4 in the router-to-router technique); ISATAP (creates tunnels that connect hosts to servers through the IPv4 network that has the IPv6 address); and Teredo (allows IPv6 traffic through NAT, from the encapsulation of the IPv6 packet into UDP packets).

2.3 NAT64/DNS64 Translation

The NAT64/DNS64 translation technique refers to the stateful method, that is, translation of IPv6 packets into IPv4 and vice versa. According to Moreiras (2012), DNS64 is a tool that directs NAT 64 in the process of synthesizing the AAAA record for the A record. These two tools, according to the author, are used together to allow the client to use the IPv6 can communicate with the server that only uses version 4 or, also, a node of this version.

According to Machado (2015), NAT 64 allows simultaneous sharing of IPv4 addresses, and uses DNS64 as an auxiliary tool for mapping domain names. In this sense, IPv6-only hosts access IPv4 devices through translation mechanisms, setting themselves up as a transparent process for the user.

Within the translation process, all version 4 addresses are mapped to the access provider's network for a predefined version 6 prefix, and can even be defined by operators. However, according to Machado (2015), in RFC 6052 there is a block of addresses that are reserved exclusively for the 64:ff9b::/96 purpose.

Thus, when a host of version 6 needs to access the contents of the same version, it will have a right access, unlike when it needs to access the contents of version 4, which performs a query to the DNS, which makes the mapping of the domain names IP. Hence, the translation technique, within the process of migration from IPv4 to IPv6, allows the equipment that uses version 5 to be able to communicate with the others that use version 4 by means of the conversion of the packages.

2.4 Other Transition Techniques

According to IPv6.br (2016), the main transition techniques from IPv4 to version 6 are the tunneling, double stack and translation, described in the previous items. According to the literature, these techniques have numerous categories that vary according to the need at the time the transition will be carried out, so they are considered to be the most relevant to the process (CORDEIRO, 2014).

According to research carried out, these categories can be described as follows:

- *Dual Stack Lite (DS-Lite)*: is a simplified Dual Stack method with RFC 6333 standardization. It applies in situations where the provider has a native version 6 network as well as the offer to users. Thus, the user has native access to IPv6, but not to IPv4 (MINELLI, 2017);
- *IVI, dIVI and dIVI-pd*: are used for providers that provide access to version 4 for users, even if there is no addressing. In this context, the stateless technique is used based on the double translation of the packages (MUNHOZ et al, 2017);
- *4rd*: Similar to the DS-Lite technique, this method, according to Minelli (2017), uses 4in6 tunnels to provide IPs within version 4 in a shared way, mainly for users who have native IPv6;
- *6PE and 6VPE*: it is often used in networks that have greater Internet connectivity. For Munhoz et. al. (2017), this technique allows the networks of version 6 to communicate through a MPLS core of version 4, using, for this, the LSPs (MINELLI, 2017);

- *6rd*: According to Miranda (2018), this technique has the purpose of allowing the user to be able to have a connection with IPv6 networks even if the network continues to work in IPv4;
- *ISATAP*: Acronym for Intra-Site Automatic Tunnel Addressing Protocol, is a technique of the tunneling category, in which it connects the devices to the routers. Usually used within companies, as they do not have a public ISATAP service (IPv6.br, 2016);
- *A + P*: Like NAT64, this technique, according to IPv6.br (2016), can be used in communion with native IPv6 deployment, ensuring that version 4 connectivity remains active for users.

As noted, the techniques described are part of the Dual Stack, Tunneling and Translation classification, which justifies the importance of understanding the functioning of these three categories within the transition process from version 4 to version 6 of the protocol.

3 Reflections on the use of the Main Techniques

Given the notes that were described in the course of this study, it was observed that all existing IPv4-to-IPv6 transition techniques are part of the common classification, namely tunneling, double-stack and translation. In this context, the study focused on addressing these items in order to promote a greater understanding and understanding about them.

According to research conducted by Machado and Rall (2016), Muniz et. al. (2017) and Miranda (2018), the consensus about this categorization is unanimous, since these authors also describe these three methods as being the main and most relevant within the transition process.

Each of the techniques cited as main have different strands and forms to be established in the transition process. Not aiming to exhaust the studies on them, this study promoted a descriptive survey of the techniques to establish the main purpose of each, a factor that allows the reader to perceive the differences between them, and in which contexts can be used, allowing users to be efficiently met within the transition.

According to Miranda (2018), each technique has advantages and disadvantages. Regarding the double-stack technique, the author points out that the advantage is in the possibility of the coexistence of versions 4 and 6 simultaneously, which allows greater ease of access to users. According to Minelli (2017), Double Stack is one of the techniques most used in the transition, and is considered as a standard technique since the new network elements can be addressed in version 6 and those that already exist can be migrated without causing major impacts to users.

In the disadvantage field, Galego and Garcia (2016) point out that Dual Stack can not be adopted when version 4 is no longer available at the provider, nor when there is no equipment that supports the operation of the two protocols at the same time.

On the tunneling technique, Miranda (2018) and Muniz et al. (2017) point out that the advantage is in the sphere of the isolation of the routing of the VPN of the normal routing, allowing to use the addresses coming from a certain VPN. According to the authors, the disadvantage of this technique can be described as compromising the security of private network information at the point of interconnection between routing.

For Miranda (2018), the translation technique is to allow the communication of the devices that have version 6 with those that use IPv4, performing an effective conversion of the packages. In the context of disadvantage, Machado and Rall (2016) say that it can be understood as the compromise of end-to-end connections, as well as their cost, since it requires equipment with great processing power.

It is worth noting that the Double Stack technique, given its permission to coexist between the two protocol versions, is the most used in the transition process. Regarding this, Miranda (2018) states that this technique should be used whenever possible, in order to avoid damages and impacts for users who use the internet protocols.

Because there is a considerable variety of transition techniques, some scholars point out the importance of adopting certain criteria in the process of IPv6 deployment, preferring IPv4 pro-lifers without the concurrent adoption of version 6, to analyze the suitability of the technique within of the network where it will be applied, verify the support of the equipment for each technique, among others (GALEGO; GARCIA, 2016, MINELLI, 2017; MACHADO, 2015).

In this context, according to Muniz et al. (2017), Dual Stack enables broad support for version 6 deployment, since many programs still only use IPv4. Thus, the option for this transition technique becomes the most indicated because it allows devices and routers to be readily equipped with batteries for both protocols.

Conclusions

This study aimed to illustrate the main characteristics of the existing transition techniques for the migration of the IPv4 protocol to IPv6, as well as to address the importance of making this change in a gradual way. For a better understanding about the theme, we tried to describe the most relevant differences of these protocols, as well as the possibilities offered by the new version 6 mechanism.

With the expansion of Internet access, the IP protocols of networked users have become scarce, making the IPv4 protocol no longer sufficient to address the amount of addressing required. In this context, it was observed that given the 32-bit capacity, the IPv4 protocol allowed the creation of a limited number of addresses, thus not meeting the necessary demand.

In order to solve this impasse, a protocol version with a larger capacity, 128 bits, was developed, which allows a greater number of addresses for networked users on the Internet.

With the purpose of increase understanding of the new IPv6 protocol, the main features of ICMPv6, Neighborhood Discovery and Stateless Addressing were described in this work, since they are fundamental for the process to occur uniformly and obtain positive results.

However, according to the researches that were carried out for this study, it was pointed out that the techniques of double stack transition, tunneling and NAT64 / DNS64 translation have important differences, being the use of each of them indicated for a certain purpose, factor which contributes to the transition does not cause major problems for users.

Thus, this study lists the characteristics of each of the transition techniques, as well as their advantages and disadvantages, increasing the understanding of each one's work and composition, contributing to a broad understanding of how the transition should to occur. Based on this assumption, he emphasized that the Dual Stack technique is the most suitable for the transition of the protocols, since it is considered one of the most complete because it allows the simultaneous coexistence of IPv4 and IPv6.

Therefore, the conclusions presented in this study, given the objectives and the proposed problems, aim to contribute to the understanding of the importance of the transition and to the emergence of new research on how techniques can be implemented, given that with the technological advance, new tools are constantly emerging to make life easier for networked users, given that the Internet is a tool that is part of the daily lives of the vast majority of people.

References

APARECIDO, A. **IPv6 na Prática**. São Paulo: Linux New Media, 2012.

BRITO, S. H. **IPv6:** o novo protocolo da internet. São Paulo: Novatec, 2013.

CISCO. **Implementing DHCP for IPv6**. 2013. Disponível em <http://www.cisco.com/en/US/docs/iosxml/ios/ipv6/configuration/15-2mt/ip6-dhcp.html>. Acesso em: 20 dez. 2018.

COLCHER, S. et al. **VoIP:** voz sobre IP**.** Rio de Janeiro: Elsevier Editora, 2005.

COMER, D. E. **Interligação de Redes com TCP/IP:** princípios, protocolos e arquitetura. 5. ed. Rio de Janeiro: Elvesier, 2005. V. 1.

CORDEIRO, E. S. **Comparação de Técnicas de Transição do IPv4 para o IPv6.** 2014. 94 f. Dissertação (Mestrado em Engenharia de Computação) - Instituto de Pesquisas Tecnológicas do Estado de São Paulo – IPT, São Paulo, 2014. Disponível em: <https://www.ipt.br/pos_graduacao_ipt/solucoes/dissertacoes/929-comparacao_de_tecnicas_de_transicao_do_ipv4_para_o_ipv6_.htm.> Acesso em: 17 dez. 2018.

FILIPPETTI, M. A. IPv6: O Futuro do Pretérito. **Admin Magazine - Redes & Segurança**, São Paulo, v. 1, n. 2, p. 10-11, jun. 2011. Disponível em: http://www.linuxnewmedia.com.br/admin/article/ipv6_o_futuro_do_preterito. Acesso em: 17 dez. 2018.

GALEGO, N. M. C.; GARCIA, N. M. **Desafios de Segurança em uma Transição de IPv4 para IPv6.** 2016. Disponível em: http://revista.apsi.pt/index.php/capsi/article/download/457/425.> Acesso em: 14 fev. 2019.

HEIDRICH, A. **Implementando um mecanismo de Transição IPv4-IPv6.** 2011. 40 p. Monografia (Especialização em Configuração e Gerenciamento de Servidores) - Universidade Tecnológica Federal do Paraná, Curitiba, 2011. Disponível em: <http://repositorio.roca.utfpr.edu.br/jspui/bitstream/1/396/1/CT_GESER_1_2011_05.pdf>. Acesso em: 8 dez. 2018.

IPV6.BR. **Transição.** Artigo do site IPv6.br. 2012. Disponível em: <http://ipv6.br/post/transicao/>. Acesso em: 18 dez. 2018.

MACHADO, L. S. **Análise dos Métodos de Transição para o Protocolo IPv6.** 2015. 69 f. Trabalho de Conclusão de Curso (Graduação em Redes de Computadores) - Colégio Técnico Industrial de Santa Maria, Universidade Federal de Santa Maria, Santa Maria, 2015. Disponível em: <http://www.redes.ufsm.br/docs/tccs/Leticia-Machado.pdf>. Acesso em: 11 dez. 2018.

MACHADO, C. N.; RALL, R. Implementação e Impacto Previsto nos provedores Regionais com a Migração do IPv4 para IPv6. In: JORNADA CIENTIFICA E TECNOLOGICA DA FATEC, 5., **Anais...** Botucatu, 2016. Disponível em: <http://www.fatecbt.edu.br/ocs/index.php/VJTC/VJTC/paper/view/862/924.>. Acesso em: 14 fev. 2019.

MINELLI, D. A. S. P. **Transição IPv4/IPv6 utilizando a Técnica Pilha Dupla.** 2017. 56 f. Trabalho de Conclusão de Curso (Graduação em Redes de Computadores) - Universidade Tecnológica Federal do Paraná, Curitiba, 2017. Disponível em: <http://repositorio.roca.utfpr.edu.br/jspui/bitstream/1/9936/1/CT_COTEL_2017_2_02.pdf.>. Acesso em: 14 fev. 2019.

MIRANDA, L. F. **Estudo da Aplicação das Técnicas de Transição e Coexistência entre Redes IPv4/IPv6 na Rede do ICEA.** 2018. 67 f. Trabalho de Conclusão de Curso (Graduação em Ciência da Computação) – Universidade Federal de Ouro Preto, Ouro Preto, 2018. Disponível em: <http://www.monografias.ufop.br/handle/35400000/1336?mode=full.> Acesso em: 14 fev. 2019.

MOREIRAS, A. M. **1% dos usuários brasileiros com IPv6.** 2012. Disponível em**:** <http://ipv6.br/um-porcento-dos-usuarios-brasileiros-com-ipv6/>. Acesso em: 4 jan. 2019.

MUNIZ, A. H. A. et. al. Estudos de Caso Transição do Protocolo IPv4 para IPv6. **Revista Gestão em Foco.** Edição 9, 2017. Disponível em: <http://unifia.edu.br/revista_eletronica/revistas/gestao_foco/artigos/ano2017/055_estudo8.pdf.> Acesso em: 14 fev. 2019.

SANTOS, L. C. dos. **Convergência entre IPv4 e IPv6.** 2013. 87 f. Trabalho de Conclusão de Curso (Graduação em Engenharia da Computação) - Centro Universitário de Brasília, Brasília-DF, 2013. Disponível em: <http://www.repositorio.uniceub.br/bitstream/235/3859/1/Leonardo%20Conde%20Monografia%201_2013.pdf>. Acesso em 09 dez. 2018.

SANTOS, R. R. et al. **Curso IPv6 Básico.** São Paulo: Ceptro.Br., 2010.

SILVEIRA, A. M. da. **Rede IPv6 com Integração IPv4.** 2012. 57 f. Trabalho de Conclusão de Curso (Tecnólogo em Nome do Curso) - Centro Federal de Educação Tecnológica de Santa Catarina, Santa Catarina, 2012. Disponível em: <https://wiki.sj.ifsc.edu.br/wiki/images/e/e3/TCC_AndreManoeldaSilveira.pdf>. Acesso em: 12 dez. 2018.

WHAT-WHEN-HOW, 2018. Available at: <http://what-when-how.com/ipv6-for-enterprise-networks/transition-mechanisms-ipv6-part-1/>. Accessed on: June 20, 2018.