DOI: 10.5604/20830157.1093208

IPv6 PROTOCOL - CHARACTERISTICS AND SUGGESTED METHODS OF IMPLEMENTATION IN EXISTING IPv4 NETWORKS USING CISCO ROUTERS

Piotr Kowalik
University of Life Science in Lublin, Information Technology Student's Scientific Club

Abstract. *The article constitutes an introduction to IPv6 protocol and is a review of the existing approaches to ensure the coexistence of IPv6 and IPv4, on the example of homogeneous Cisco network infrastructure. In the first paragraph, the IPv6 protocol has been characterized and compared to the IPv4. Then, concepts connected with IPv6 addressing have been described. As the main part, it has been discussed methods to provide the coexistence of the two IP protocols. It has been characterized the primary option which is the dual stack, two types of both point to point and multipoint tunnels and finally - address translation NAT-PT.*

Keywords: computer networks, IP networks, protocols

PROTOKÓŁ IPv6 - CHARAKTERYSTYKA I PROPONOWANE METODY WDROŻENIA W ISTNIEJĄCYCH SIECIACH IPv4 KORZYSTAJĄCYCH Z ROUTERÓW CISCO

Streszczenie. *Artykuł stanowi wprowadzenie do protokołu IPv6 oraz jest przeglądem istniejących podejść dla zapewnienia współistnienia IPv6 i IPv4, na przykładzie homogenicznej infrastruktury sieciowej Cisco. W pierwszym rozdziale scharakteryzowano protokół IPv6 i porównano go z IPv4. Następnie opracowano koncepcje związane z adresowaniem IPv6. W głównej części opisano metody do zapewnienia koegzystencji dwóch protokołów IP. Scharakteryzowano podstawową opcję jaką jest podwójny stos, po dwa rodzaje tunelowania punkt-punkt i punkt-wielopunkt oraz w końcu translację adresów NAT-PT.*

Słowa kluczowe: sieci komputerowe, sieci IP, protokoły

Introduction

Widespread use of computer networks and rapid growth of the Internet in recent years has caused the exhaustion of IPv4 addresses. Despite use of various techniques aimed at economical use of available pool, such as NAT, depletion of available addresses could not be avoided, but only moved in time. This situation has induced intensification of interests in IPv6 protocol. This protocol both increases available amount of addresses and also introduces several important changes in comparison to well-known IPv4 [1].

Migrating billions of computers and other network devices from IPv4 to IPv6 is not possible immediately. This process will take many years and knowing that, network equipment manufacturers have developed tools that allow coexistence of two versions of IP, both on the Internet and in local area networks. Cisco - one of the largest manufacturers of network devices - in IOS operating system, used by routers and switches, has implemented a number of interesting methods to ensure smooth functioning of both IPv4 and IPv6. These methods are: dual stack, point to point tunneling (manually configured tunnels and GRE tunnels), point to multipoint tunneling (6to4 tunnels or ISATAP tunnels) and NAT-PT mechanism [2].

In the article have been discussed important issues of transitioning from IPv4 to IPv6, which many companies will have to deal with. In the first part, the IPv6 protocol has been characterized and compared to the IPv4. Also, concepts connected with IPv6 addressing have been described. In the second part it has been discussed methods to provide the coexistence of the two IP protocols. It has been characterized the primary option which is the dual stack, two types of both point to point and multipoint tunnels and finally - address translation NAT-PT.

1. IPv6 protocol

1.1. Differences between IPv6 and IPv4

An IPv4 address is 32 bits long and is represented by decimal characters. An IPv6 address is 128-bit binary value and can be written as 32 hexadecimal characters. Apart from this fundamental difference connected with providing a sufficiently large number of available addresses, IPv6 introduces many improvements and enhancements in comparison to its precursor. The most important are: addressing reformation, simplification of the header being added in an encapsulation process, improved security issues and a wide range of migration strategies [1].

Table 1. IPv4 and IPv6 – a short comparison

	IPv4	IPv6
Address size	32 bits	128 bits
Address example	192.168.10.101	2001:db8a::3257:9652
Number of address	4.294.467.295	$3{,}4*10^{38}$
Header size	20 octets	40 octets
QoS	Type of service field	Flow label field
Control messages	ICMP	ICMPv6
Checksums	Present	Moved to data link layer
Address configuration	Manual or DHCPv4	Manual, DHCPv6 or auto-configuration

Reformed addressing means no broadcast messages, ability to have multiple IPv6 addresses on a single physical link, which increases the reliability of connections and also auto-configuration with use of data link layer address. The simplification of the header has been realized by reducing number of fields to 8 and simultaneous increasing of its size to 40 octets (see Fig. 1). Smaller number of fields and no need for processing checksums allows to increase efficiency of routing [2].

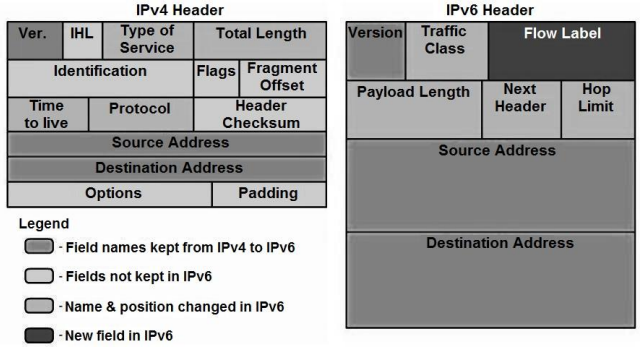

Fig. 1. IPv4 and IPv6 headers [2]

1.2. IPv6 addressing concepts

As mentioned before, an IPv6 address is 128-bit binary value, being written as eight groups of 16-bit values separated by colons. IPv4 addresses had fixed notation. The IPv6 addresses does not require a complete disclosure. It can be shortened according to certain rules. An example of IPv6 address and the way of shortening it is shown in Fig. 2 [2].

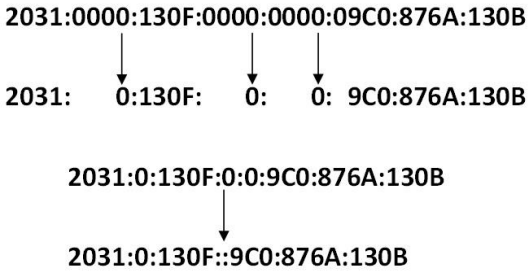

Fig. 2. Method of IPv6 address shortening [2]. In the first phase leading zeros have been removed. In the second phase, neighboring fields made up of zeros have been replaced by two colons

In general, there are two rules. First, says that the leading zeros in a field does not require to be written (e.g. field 0000 can be written as 0 or 08B1 can be written as 8B1). The second - successive fields composed of zeroes can be replaced by two colons (this method can be used only once). The rules allows to significantly reduce the size of most addresses [2].

IPv6 addresses can be divided into several major groups:

- global unicast addresses (see Fig. 3), which are equivalent to IPv4 public addresses. Each address consists of 48-bit global routing prefix and 16-bit subnet field. Last 64 bit is an interface identifier (identifies a host). These addresses start from 2000::/3.
- private addresses, which are not transferred outside the local network (e.g. local-link addresses (see Fig. 4), start with FE8, FE9, FEA or FEB)
- loopback address - 0:0:0:0:0:0:0:1 (::1), designed for tests, equivalent to 127.x.x.x IPv4 addresses group.
- unspecified address - 0:0:0:0:0:0:0:0 (::), used when sending device does not know its own address
- group addresses – start from FF::/8, used for example by routing protocols like RIP or EIGRP
- special reserved addresses - e.g. group of addresses for described 6to4 tunneling

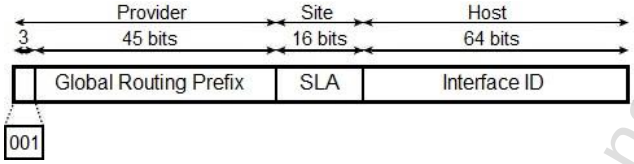

Fig. 3. Global unicast address scheme [5]

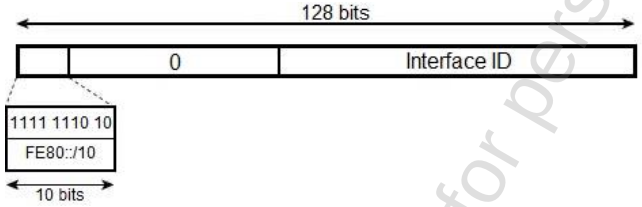

Fig. 4. Local-link address scheme [4]

2. Methods to ensure the coexistence of IPv4 and IPv6 protocols

Move from lack of IPv6 support to full support of this protocol does not occur instantaneously. In large companies, this process starts with moving to IPv6 only several routers, servers and hosts. Over time, number of devices switched to the new protocol in the organization begins to grow and at some point, IPv6 will completely replace IPv4 and support of this protocol will be disabled. Process of this gradual transition will last many years. The smooth transition to IPv6 is possible by three groups of tools [3]:

- Dual stack
- Tunneling
- NAT-PT

2.1. Dual stack

Primary and most commonly used method for the coexistence of IPv6 and IPv4 in a network is the dual stack (see Fig. 5). It consists in configuration of IPv6 routing protocols and IPv6 addresses on all routers and hosts in a network, that have to forward IPv6 packets. A dual-stack device chooses which stack to use based on the destination address of the packet. If IPv6 is available, then a dual-stack host should prefer it for communication. IPv4-only applications continue to work as before. New and modified applications can use both IP layers [2].

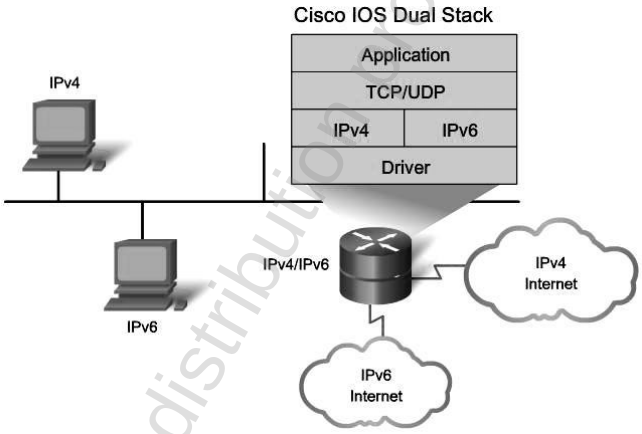

Fig. 5. Basic concept of the Dual Stack [2]

In the future the aim should be to ensure full coexistence of both versions of the IP protocol and then building new networks based only on IPv6, however this will be a long term process. At the present in many large networks there is a need to allow IPv6 communication for only a specific group of hosts or due to size of a network, simultaneous enabling IPv6 support is a problem. For such cases have been developed methods based on encapsulation of an IPv6 packet in an IPv4 packet [3].

2.2. Point to point tunnels

Tunneling is the process of encapsulation an IPv6 packet in an IPv4 packet by the router. The packet is treated by consecutive devices as a normal IPv4 unit and last router on the way de-encapsulates it and sends to its final destination. Tunneling does not require configuring IPv6 throughout the network, what allows to quickly provide IPv6 connectivity only in this part of the network, which needs it. The general concept of tunneling is shown in Fig. 6 [3].

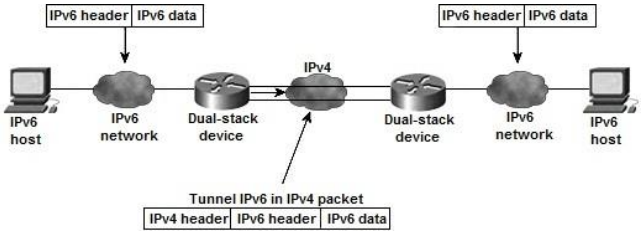

Fig. 6. General concept of tunneling [6]

A characteristic feature of point to point tunnels is that only one device can be located at each side of a tunnel. For each pair of IPv6 hosts, which have to communicate with each other, it is necessary to create a separate tunnel. Routers on the end of a tunnel treat the tunnel interfaces as serial point to point links [3].

The two available types of point to point tunnels are MCT (Manually Configured Tunnels) and GRE tunnels (Generic Routing Encapsulation). These tunnels connects many similarities: both use virtual point to point link to transmit packets, in both

cases it is possible to configure IPv6 IGP routing protocols on these virtual links and finally in both methods it is necessary to set up the source and destination IPv4 addresses of the tunnel statically. The difference is greater flexibility of GRE tunnel, which can be understood as the ability to send many passenger protocols and the use of transport protocols (encapsulating passenger protocols) other than IPv4. Sending passenger protocols is possible due to additional header placed between IPv6 and IPv4 headers [2, 3].

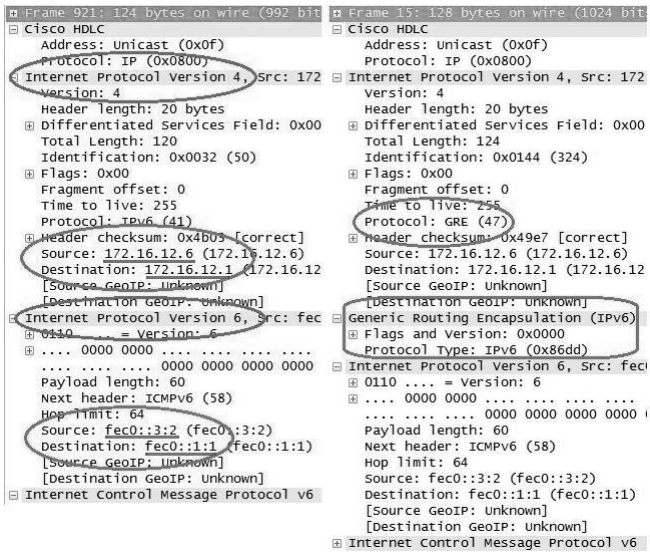

Fig. 7. Comparison of frames outgoing from router with tunneling enabled. MCT on the left, GRE on the right side; In both cases an IPv6 packet is encapsulated in an IPv4 packet. The source and destination IPv4 addresses, added to the IPv4 headers, are known from configuration of the tunnels. The only difference – GRE has an additional header between the IPv4 and the IPv6 header

Basic configuration of point to point tunnels is relatively simple. It consists in selection of IPv4 addresses, that will be used as the source addresses for the two routers, between which an IPv6 connectivity has to be established. Next step is to create tunnel interfaces on both routers and assign them source and destination IPv4 addresses. Finally, according to the needs, to select the mode of the tunnel (MCT or GRE) and to assign IPv6 addresses to external router interfaces between which an IPv6 link has to be provided [3, 4].

2.3. Point to multipoint tunnels

When IPv6 traffic is occasional and its size is difficult to predict, point to multipoint tunnels can be a good solution. These tunnels allow a single router to send packets to multiple routers with use of a single tunnel interface. The encapsulation process is similar to previously mentioned point to point tunnels. The main difference is the addition of an essential information, which allows a sending router to direct packets to an appropriate destination. The destination IPv4 address of the tunnel is embedded in the destination IPv6 address of the packet. To allow this concept to work, an appropriate addressing plan is required, which in turn depends on the selected multipoint tunnel type [3].

In the multipoint topology, under certain conditions, new devices can be connected to the tunnel without performing additional configuration on existing routers, what can be considered as an advantage. Moreover, this type of tunnels, in contrast to point to point tunnels, do not support IGP IPv6 routing protocols and thus require the use of static routes or BGP. Their use is also associated with a dynamic transmission of each packet, which in turn uses relatively a lot of router resources. Furthermore, multipoint tunnels configuration method are slightly more complicated in comparison to the previously described methods [3].

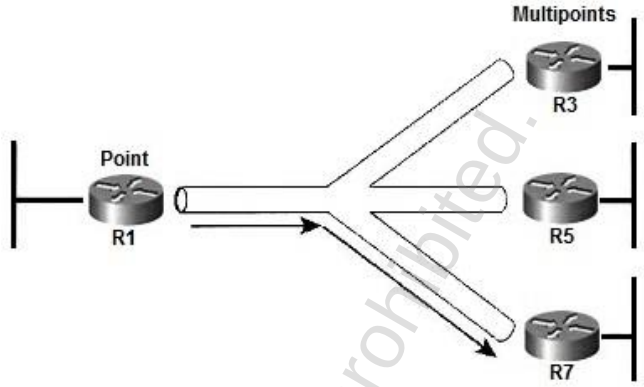

Fig. 8. Concept of point to multipoint tunneling [3]

There are two main methods of multipoint tunneling: automatic 6to4 tunnels and ISATAP tunnels. To use the 6to4 tunnel it is necessary to decide while planning, whether global unicast IPv6 addresses or special reserved block of IPv6 addresses starting from 2002::/16 are applied. If all traffic from the Internet to the organization uses IPv4 only, then the use of the reserved address range is recommended. It simplifies the configuration process and allows to exploit advantage of the multipoint tunnels, which is the ability to add new hosts without reconfiguring existing routers. On the other hand, if the company needs to apply IPv6 addresses for Internet connections, the use of global unicast addresses is indispensable. The important thing is how router determines to which endpoint of the tunnel to send the packet. In case of using the reserved block of IPv6 addresses, the source and destination addresses of the tunnel are stored in second and third quartet of the source and destination IPv6 addresses, converted to hexadecimal values. For example, the packet sent from the host with IPv6 address 2002:AC10:C06:3::1/64 to IPv6 2002:AC10: C01::1/64, when reaches the tunneling router, receives an IPv4 header with 172.16.12.6/30 source address, and will be directed to 172.16.12.1/30 destination address. These addresses have been determined by converting AC10:C06 and AC10:C01 form hexadecimal to decimal representation. In this way, the proper router can receive a packet and, after removing of IPv4 header, send it to the target IPv6 host. The situation is different when using global unicast addresses. Encoding the source and destination IPv4 addresses in IPv6 addresses is not possible because IPv6 addresses are allocated to the company by the external organization. This problem is solved by recursive route search by the router forwarding packets through its tunnel interface. In practice, it means the need to define specific static routes for the tunnel interface and this in turn brings more work when topology is changed [3, 4].

The second method of multipoint tunneling is ISATAP (Intra-site Automatic Tunnel Addressing Protocol). This concept, in some points, is similar to previously described 6to4. The tunnel interfaces use IPv6 addresses, in which IPv4 addresses are embedded and there is a necessity to configure static routes to the endpoints. In contrast to 6to4, destination IPv4 address is placed in seventh and eight quartet of IPv6 address. Also, there is no possibility of using reserved block of addresses and all tunnel interfaces use IPv6 prefixes from the same subnet. In addition, these tunnels can build interface identifier on the basis of network card MAC address (modified EUI-64). The tunneling router determines destination of the IPv6 packet by searching routes, previously added to its routing table. After receiving the packet, router checks the next hop IPv6 address for a matching route, and knowing that ISATAP is the used tunnel mode, it looks for destination IPv4 address in the last two quartets of found next hop address. This IPv4 address will be inserted into an additional header and the packet will be treated as an usual IPv4 packet by all routers on the way to the destination [3].

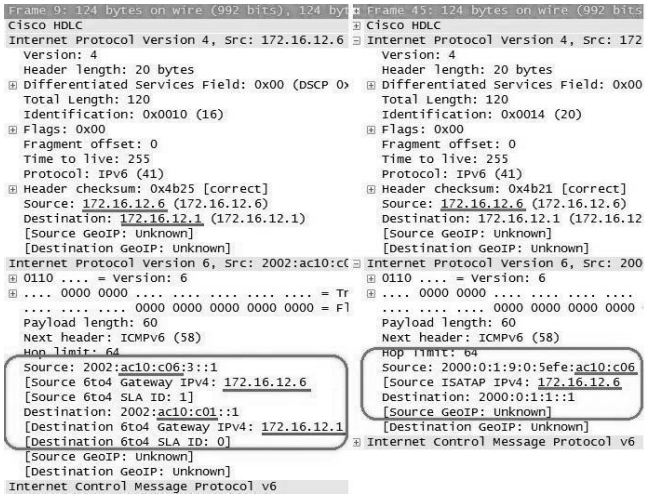

Fig. 9. Comparison of frames outgoing from router with 6to4 (on the left) and ISATAP (on the right) configured; 6to4 IPv4 addresses are known from second and third quartets of IPv6 addresses. ISATAP source IPv4 address is determined from seventh and eight quartets of IPv6 source address (destination IPv4 address is determined on the basis of next hop address of a matching static route)

2.4. NAT-PT

In some situations, at the stage of transition to IPv6, there is a need to ensure communication between hosts with different types of IP protocols support. For such cases has been developed a mechanism called NAT-PT (Network Address Translation-Protocol Translation). This method is similar to well known NAT, which has been helping to spare IPv4 addressing space, by translating private addresses to public for Internet connections. NAT-PT consists in translation source and destination addresses, along with whole headers, from IPv4 to IPv6 and vice versa [3].

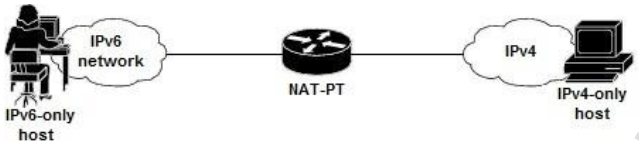

Fig. 10. Basic NAT-PT concept [7]

The configuration of NAT-PT is performed on the router by assigning to a given IPv4 address, an IPv6 address, to which it has to be converted when a packet is destined to an IPv6 host. Likewise for communication in the other direction (Fig. 11). For example, when the host with IPv6 address FEC0::3:2 tries to send a packet to an IPv4 host 10.1.3.2, it reaches first a router with IPv6, on which translation has been configured. Then the router converts the IPv4 header, simultaneously substituting the source and destination addresses with appropriate ones. The substituted source address is pre-configured on the router for translation purposes, destination address is IPv4 host address, in this case-10.1.3.2. It works analogously with the traffic sourced from the other direction [3].

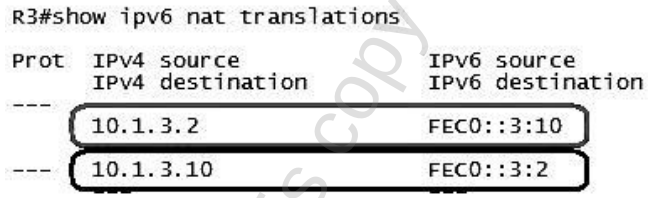

Fig. 11. Show ipv6 nat translation command on Cisco router for configured NAT-PT; Source IPv4 address 10.1.3.2 is translated to FEC0::3:10. Source IPv6 address FEC0::3:2 is translated to 10.1.3.10

3. Summary

Complete disappearance of IPv4 protocol is not possible in the near future. Over the coming years it is expected that both IPv4 and IPv6 protocols will coexist in the networked world. Despite the variety of methods for ensuring the coexistence of IP protocols, the use of dual stack should be always considered at first. Even in case of initial rejection of this solution for tunneling, finally the dual stack must be the method to deploy and other methods should be exploited temporarily [3].

In case of choosing the concept of tunneling, advantages and disadvantages of available options should be considered to select proper way to meet the needs. The first thing to keep in mind is that every kind of tunneling consumes more router resources on which it is performed (in comparison to the dual stack). It is the result of additional encapsulation and de-encapsulation of packets. Point to point tunnels are good choice when regular and large traffic is expected on the tunnel interfaces. It is connected with no need to take dynamic decisions by the router to determine destination of the packets and therefore the router load is lower. In addition, configuration process of point to point tunnels is simple and does not require extensive knowledge. Point to multipoint tunnels are appropriate when expected IPv6 traffic is occasional or its size is difficult to predict. The tunneling router forwards the packets dynamically, based on various, depending on the tunnel type rules. The advantage of multipoint tunnels is the ability to add new hosts to the tunnel without performing any additional configuration on existing routers, but this require an appropriate addressing design and can be troublesome in certain situations [3].

The specific method is NAT-PT. It is applied when there's a need to provide connection between devices with different types of the IP protocol. One of the benefits of address translation is that no reconfiguring of existing hosts is required, because all the configurations are performed at the NAT-PT router. NAT-PT should not be used when other native communication technique is possible to apply [7].

The article does not exhaust the subject of the IP protocols and its coexistence. It constitutes only a sort of introduction and familiarization the Reader with IPv6 protocol and its implementation approaches on the example of Cisco networks. Wider descriptions and more detailed explanations of the described concepts can be found in Cisco technical documentations, which were also used while creating this article.

References

[1] Dye M., McDonald R., Rufi A.: Network fundamentals, Cisco Press 2008.
[2] Graziani R., Vachon B.: Sieci WAN - zasady dostępu, PWN, Warszawa 2012.
[3] Wendell O.: CCNP Route - Oficjalny przewodnik certyfikacji, PWN, Warszawa 2013.
[4] http://www.cisco.com/en/US/docs/ios-xml/ios/ipv6/configuration/12-4t/ip6-tunnel.html
[5] http://www.cisco.com/en/US/docs/ios-xml/ios/ipv6/configuration/12-4t/ip6-addrg-bsc-con.html
[6] http://www.cisco.com/en/US/docs/ios-xml/ios/interface/configuration/xe-3s/ip6-man-tunls-xe.html
[7] http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-nat_trnsln_ps6350_TSD_Products_Configuration_Guide_Chapter.html

Eng. Piotr Kowalik
e-mail: pk82192@up.edu.pl

Student of second degree studies at the Faculty of Production Engineering at the University of Life Sciences in Lublin. Chairman of the Information Technology Student's Scientific Club functioning at the Department of Mathematics and Information Technology Applying. Active participant of scientific conferences. Cisco CCNA certificate holder. Interested in administrating computer networks and programming in Java and C++ languages.

otrzymano/received: 26.07.2013 *przyjęto do druku/accepted: 10.01.2014*