The Plan for Migration to IPv6 in the Academic Network of the University of Montenegro With Examples of Implementation

Miodrag Zarubica[1], Vladimir Gazivoda[2], Ljiljana Adžić[3], Luka Filipović[4], Božo Krstajić[5]

***Keywords**: IPv6, Dual Stack, IPv4, transition*

Abstract: This paper presents a migration plan to the IPv6 protocol in the Academic Network of the University of Montenegro, with application examples in the Center of Information System (CIS) and in the network of the Faculty of Electrical Engineering. The migration procedures, the plan of the recommended migration model from IPv4 to IPv6 and Dual Stack technology, and its advantages are explained and discussed. The concept of segmentation of the new IPv6 address range and migration of public services to the new IP protocol is also presented.

1. INTRODUCTION

With the development of the Internet as a global computer network, the expansion of its availability, and the emergence of an ever-increasing number of applications and services, the number of Internet users is increasing daily. Along with the increased number of users, we witness the increasing need for public IP addresses, the number of which is approaching the total number of available addresses. Therefore, a solution had to be sought for a new protocol that would contain a larger range of IP addresses capable of meeting the needs of the new Internet. A new IPv6 protocol has been developed that uses a 128-bit address for device addressing.

Major web companies like Google, Yahoo, and Facebook started using IPv6 protocol addresses in 2011 for the purpose of testing, while 2012 is considered the first year of official use of IPv6 protocol [1]. Although necessary, the implementation of the IPv6 protocol did not exceed 1/3 of Internet hosts by the beginning of 2021 [2].

[1] Miodrag Zarubica, Center of Information System, University of Montenegro, Cetinjski put br. 2, 81000 Podgorica, Montenegro (e-mail: miodrag@ucg.ac.me);

[2] Vladimir Gazivoda Center of Information System, University of Montenegro, Cetinjski put br. 2, 81000 Podgorica, Montenegro (e-mail: vladg@ucg.ac.me);

[3] Ljiljana Adžić, Center of Information System, University of Montenegro, Cetinjski put br. 2, 81000 Podgorica, Montenegro (e-mail: ljilja@ucg.ac.me);

[4] dr Luka Filipović, Center of Information System, University of Montenegro, Cetinjski put br. 2, 81000 Podgorica, Montenegro (e-mail: lukaf@ucg.ac.me);

[5] Prof. dr Božo Krstajić, Faculty of Electrical Engineering, University of Montenegro, Cetinjski put br. 2, 81000 Podgorica, Montenegro (e mail: bozok@ucg.ac.me).

Following the global development trends, the Center of Information System (CIS) of the University of Montenegro (UoM), as the administrator of the Academic Network, has included the implementation of the IPv6 protocol in its action plan. A plan for implementation was created and the segmentation of the obtained address range was performed based on the assessment of the further development of the Academic Network.

This paper describes the plan for implementation of the IPv6 protocol in the Academic Network of the University of Montenegro and practical examples of implementation in the center of the Academic Network of UoM and the connection between CIS and the Faculty of Electrical Engineering of UoM.

2. ADVANTAGES OF IPV6 PROTOCOL

The international organization ISO (International Standardization Organization) has defined the general model of communication systems as OSI (Open System Interconnection) model. OSI represents a layered model that specifies the way of communication between networks, using different protocols specified for seven layers individually (physical layer, link layer, network layer, transport layer, session layer, presentation layer, and application layer) [3].

Modern Internet-based communication networks use the Internet Protocol Suite reference model, which is a combination of protocols for different types and needs. The two main protocols in this model are TCP (Transmission Control Protocol) and IP (Internet Protocol) [4]. The TCP/IP protocol has been standardized and widely used since version 4, and the first standardized version was known as IPv4 [3], [4].

With the development and expansion of the Internet and the ever-increasing expansion and development trend that is expected to continue, deficiencies in the IPv4 protocol have been identified. To address the deficiencies and enable further expansion of the Internet, a new protocol called IPv6 was developed [3].

The IPv6 protocol is a key prerequisite for the continued development of the Internet, by expanding the address range that has reached its maximum with IPv4 which proved to be limited from the aspect of realizing the concept of the new generation of the Internet. The IPv6 increases the address range from 32 to 128 bits, thus creating the conditions to support the expected increase in the number of objects that form the basis of the Internet of Things (IoT) concept [3], [5].

By increasing the address space, it was possible to improve some IPv4 functions, as well as to add completely new functions to the IPv6 specification. The auto-configuration function has been significantly improved [3].

Unlike IPv4, IPv6 offers automatic configuration with very simple configuration mechanisms (plug-and-play). Namely, thanks to the fact that the complete IP prefix is supplied, and not just the address, the device can automatically configure its own IPv6 address and does not require server assistance. Moreover, if an IPv6 router is present, any device that supports IPv6 can generate not only a local address but also a globally routable address; thus gaining access to the global Internet. In addition to the described auto-configuration option, IPv6 also retains the DHCPv6 option, i.e. auto-configuration like IPv4 DHCP [3].

The speed of IP packet routing is increased with IPv6 networks, which is a significant advantage from the perspective of current applications and services, as well as the realization of the IoT concept [5], [3].

Compared to IPv4, IPv6 has a much simpler packet header structure designed to minimize processing time and procedures. This has been achieved by moving the option field and possibly other fields into the header extension so that the IPv6 packet header itself can be processed more efficiently by routers. Since the router does not need to check the checksum under these conditions, its software or hardware becomes simpler and enables faster packet processing, reducing the overall processing delay and thus improving the performance of the entire network [3], [4].

There are also several other reasons that pose significant challenges in networks based on the IPv4 protocol that are just being overcome by the implementation of IPv6 [3].

By introducing mandatory support for network-level security (IPSec), IPv6 nominally has a significant advantage over IPv4 where there is no source address validation since routers redirect packets based only on the destination address. By providing end-to-end protection via the IPSec protocol, IPv6 can provide applications with guarantees of the authenticity and confidentiality of exchanged data, eliminating the need for applications to implement these functionalities themselves. By using the same protection mechanisms for all applications, the implementation and administration of protection functions becomes much simpler, but reduces the flexibility in terms of the application itself [3].

User mobility presents a major challenge in networks with traditional architecture, i.e. requires an intensive and continuous increase in mobile Internet penetration [3]. With IPv6, mobility support is achieved by implementing the Mobile IPv6 (MIPv6) protocol, which has a built-in transmission path optimization function. Additional functions, such as Neighbor Discovery and address auto-configuration, allow mobile devices (nodes) to operate at any location without the need for a separate router. Thanks to the Mobile IPv6 protocol, connectivity to the transport layer is ensured, allowing the nodes to remain reachable regardless of their location in the IPv6 network. In this way, the existing connections over which the mobile node communicates are preserved, regardless of changes in its location and address [3].

Quality of Service (QoS) and traffic management have their limitations even in the traditional Internet architecture, especially when it comes to guaranteeing QoS on a priority basis and in real-time [3].

With the IPv6 protocol, the conditions for ensuring the required level of QoS have been significantly improved by the introduction of a new "Flow Label" field (FL) in the header, which defines the way in which packets are identified and handled by the router. This ensures a more efficient transfer of data from one end to the other, without allowing intermediate devices to modify it, i.e. violate the QoS level [3]. In addition to that, by using IntServ (Integrated Services) and DiffServ (Differentiated Services) type protocols, IPv6 enables the required, increased QoS, required by newer applications, such as IP telephony, video/audio, interactive gaming, or e-commerce. Unlike IPv4 which supports best-effort services, IPv6 ensures QoS in the form of a set of service requirements, that guarantee an improved level of network performance for transmission. In addition, the quality of network traffic is defined by parameters such as data loss, delay, or bandwidth. In order to implement the QoS tag, IPv6 uses the "Traffic Type" field (8 bits) in the IPv6 header, as well as the specified 20-bit "Flow Labels" field [3].

3. TRANSITION MECHANISMS IPV4/IPV6

The Internet as we know it today consists of native IPv4, IPv6 and IPv4/IPv6 dual networks. IPv4 and IPv6 are not compatible protocols. When both protocols are present on the network path, and it is necessary to ensure that Internet users can connect without any restrictions, transition mechanisms are required. Many mechanisms have been developed that enable a smooth transition from IPv4 to IPv6 networks and enable device communication in the environment with both protocols. Previously, IPv6 networks were implemented as independent network segments, while now they connect and work together with IPv4 networks [3], [6], thanks to transition mechanisms.

Different types of transitions are divided into three broad groups [3], [6]:

- dual configuration (dual stack);
- tunneling;
- translation (translation).

A. Dual stack configuration

Dual stack configuration is a mechanism that enables devices to communicate in an environment where both protocols operate in parallel, allowing network nodes to communicate using either IPv4 or IPv6 protocol. The dual configuration enables the transport of both IPv4 and IPv6 packets. The decision of which protocol to use is made based on the version and type fields of the destination IP address. Although this is the most widely used transition mechanism, it only enables the communication of similar network nodes (IPv4 with IPv4 and IPv6 with IPv6 nodes) [3], [6].

B. IPv4 - IPv6 Tunneling

This transition mechanism enables the bridging of incompatible networks. In practice, there are several variants of tunneling, which are generally divided into two categories:

- centralized – predefined, manually configured by the administrator;
- automatic - configured automatically (on the fly), based on the information contained in the IPv6 packet (e.g. source and destination IP address). There are the following automatic tunneling techniques: 6to4, Teredo, ISATAP, Tunnel brokers, 6over4, and Dual Stack Transition Mechanism (DSTM) [3], [6].

This mechanism allows an IPv6 packet to be sent over an IPv4 network. The encapsulation feature of this transition mechanism is applied to the source router or host. Encapsulation adds an IPv4 destination address, and an IPv4 source address, and 41 is entered in the protocol field in the IPv4 header - the value of the field indicates that it is an encapsulated IPv6 packet. Decapsulation is performed at the egress host to remove the IPv4 header, after which the packet is routed to the destination IPv6 address [3], [6].

C. IPv4/IPv6 translation

This transition mechanism uses translation from IPv4 to IPv6 at a specific protocol layer, usually at the network, transport, or application layer. In contrast to the tunneling mechanism, translation converts packets from the IPv4 to the IPv6 protocol and vice versa. There are several translation methods, the most popular are: SIIT, Bump in the API, Bump in the Stack, NAT-PT, and others [3], [6].

4. THE PLAN FOR IPV6 IMPLEMENTATION IN THE ACADEMIC NETWORK OF UCG

A. Dual Stack method was chosen while creating a detailed plan for the implementation of IPv6 in the Academic Network. This translation method is the widely used solution according to the experiences of network operators that have already implemented IPv6 in their networks.

From the point of view of the academic network, this method represents a solution that causes the least changes and modifications in the network, and the translation and implementation that users in the academic network will not perceive.

Moreover, while analyzing the devices that are currently working in the academic network, we found that most of the devices support IPv6. So, from a financial point of view, this method is currently the most profitable for the University of Montenegro.

B. IPv6 Address Space Segmentation (Address Range Planning).
There are several methods of address range planning, and taking into account the segment allocated to the academic network (2A02:4280://32), we have chosen the following address space categorization:

2A02:4280:ITTJ:JJ::/56

where "I" stands for institution, "T" is for type, and "J" is for organizational unit.

By choosing this categorization, we maintain enough flexibility to cover the existing network and leave room for further expansion of the network to institutions that are not currently part of the Academic Network.

Given that the Academic Network has an established IPv4 addressing scheme and all devices in the IT center and border devices by university units have IPv6 support, therefore, Dual stack represents the optimal solution for migration to IPv6 due to minor changes in configurations of network devices and user computers.

Dual stack enables parallel deployment of IPv6 addresses on existing interfaces. For example, the WAN router is configured so that all interfaces have parallel IPv6 addresses, and BGPv6 is established at the WAN provider (GEANT) [7], as well as to the local Internet Exchange Point (MIXP) [8].

Given the architecture of the academic network, which is multi-star shaped, static routes are established on all devices at the IT center. In the cases where dynamic address assignment was required, the ND protocol was enabled for the border device to propagate its IPv6 network prefix, and the devices themselves generate a part of the address for their

interfaces. In the case of the server segment, the ND protocol was not enabled, because it was necessary to set static IPv6 addresses and propagate them through DNS.

Fig. 1 shows the current architecture of the Academic Network with devices configured with IPv6 addresses [9], [10], [11].

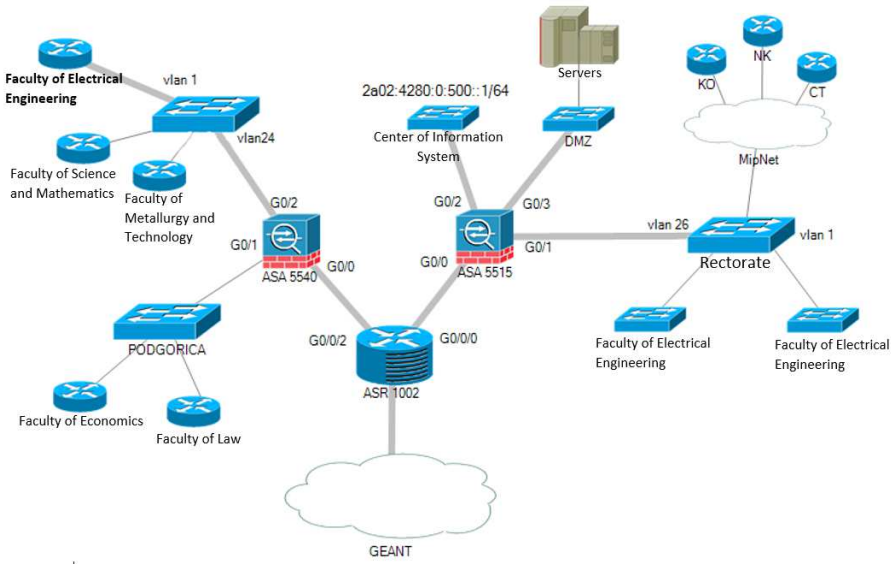


Fig. 1. Current architecture of the UoM Academic Network

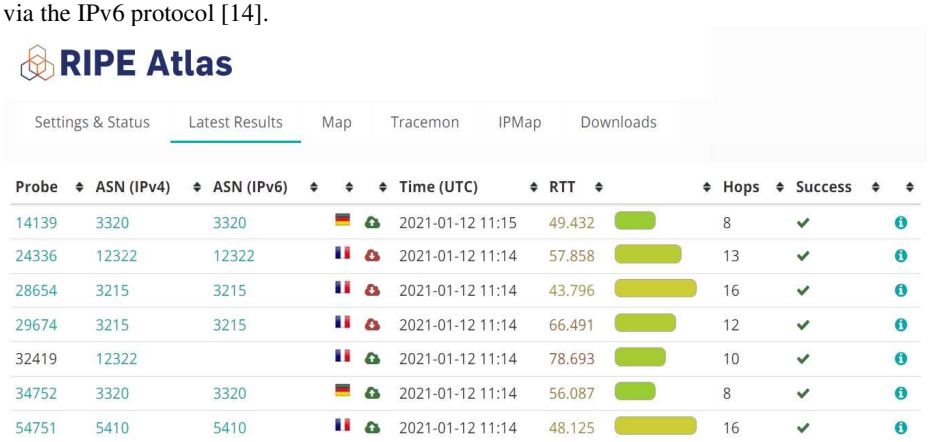
The introduction of IPv6 is fully compatible with the existing configuration of VLAN interfaces and trunk interfaces, which was very convenient for setting up IPv6 addresses in the server segment. IPv6 translation was implemented on critical services that are mostly used: DNS, MAIL, WEB.

As for the servers themselves, we get IPv6 connectivity by setting an IPv6 address on the same interface, but the service configurations also had to be adjusted and set to work over IPv6 addresses. Here we will only mention that for DNS, in addition to changing the configuration, we also added AAAA directives that resolve the domain name to an IPv6 address in the corresponding zone files [12], [13]. This enabled the existing DNS to resolve IPv6 in addition to IPv4 addresses, and to be available via the IPv6 protocol [12].

For the needs of MIXP [8], a new virtual machine was created with an instance of the BIRD service (routing service), configured to work with IPv6 addresses only. In this parallel operation, this root server operates with IPv6 addresses exclusively, while the existing root server operates with IPv4 addresses. As mentioned earlier, IPv6 does not depend on the existing configuration of VLANs and trunk interfaces, so the implementation here was performed without changing the existing device configuration.

Fig. 2 shows the RIPE Atlas traceroute test of the website www.ucg.ac.me (IPv6 address 2a02:4280::200:89:188:43:93), which indicates that there are active IPv6 addresses from

Montenegro and that the network of the University of Montenegro is visible on the Internet via the IPv6 protocol [14].



Probe	ASN (IPv4)	ASN (IPv6)	Time (UTC)	RTT	Hops	Success
14139	3320	3320	2021-01-12 11:15	49.432	8	✔
24336	12322	12322	2021-01-12 11:14	57.858	13	✔
28654	3215	3215	2021-01-12 11:14	43.796	16	✔
29674	3215	3215	2021-01-12 11:14	66.491	12	✔
32419	12322		2021-01-12 11:14	78.693	10	✔
34752	3320	3320	2021-01-12 11:14	56.087	8	✔
54751	5410	5410	2021-01-12 11:14	48.125	16	✔

Fig. 2. Visibility of the IPv6 address of the site www.ucg.ac.me - RIPE Atlas test [14]

C. Implementation of IPv6 at the Faculty of Electrical Engineering, University of Montenegro.

After the implementation at the IT center was done, we have gradually started the planned implementation of the IPv6 protocol on each university unit. First, the implementation of the new protocol was started at the Faculty of Electrical Engineering as one of the larger units of the University of Montenegro, which also has functionally separate segments in its structure and is located within the UoM campus. The implementation of IPv6 at the Faculty of Electrical Engineering is a representative example that can serve as a model for implementation in other units of the University for configuring their devices and planning IPv6 infrastructure.

The Faculty of Electrical Engineering is assigned the network address **2a02:4280:10:100::/56**. Since such a network has 256 subnets, this allows for great flexibility in configuring the internal topology.

The internal topology itself is divided into three areas: offices, laboratories/classrooms and services (student and accounting). Accordingly, the network is segmented into three parts and each part is assigned a subnet with the /64 prefix.

During the implementation of IPv6 at the Faculty of Electrical Engineering, it was noted that a significant number of public IPv4 addresses were used, and that many private IPv4 addresses were used for various purposes. This made the network administration very complicated especially the management of traffic and security policies. The implementation of the IPv6 protocol solves this problem and allows each computer to have a unique public IP address.

5. CONCLUSION

The paper presents the results of the first planned implementation of the IPv6 protocol in Montenegro, in the UoM Academic Network. A typical example of migration of a WAN network to IPv6 using dual-stack technology is shown, according to the well-known "outside-in" scenario [3]. The executive summary of the transition of UoM IT center, which is connected to the Internet (the "outside" term), as well as the example of the concept of migration of the internal unit and its computer network (the "inside" term) were presented.

The implementation examples shown in this paper, together with the Plan [3], can serve as a starting point for other ISPs in Montenegro that want to start implementing the IPv6 protocol in their networks. By implementing the IPv6 protocol, the Academic Network and UoM itself obtained a significant resource for further development and research.

REFERENCES

[1] Saša Stamenković (2012, Sep. 12). "IPv6: the die is cast!". PC PRESS [Online]. Available: https://pcpress.rs/ipv6/. [Accessed: Feb. 27, 2019].
[2] Google statistics on IPv6, adoption on the Internet, "google.com". [Online]. Available: https://www.google.com/intl/en/ipv6/statistics.html. [Accessed: Jan. 27, 2021].
[3] Agency for Electronic Communications and Postal Services, "Study on IPv6 Migration Plan in Montenegro"," ekip.me. [Online]. Available: www.ekip.me/izvjestaji/ipv6.php. [Accessed: May. 12, 2019].
[4] RFC 791 - Internet Protocol, DARPA Internet Program, Protocol Specification. [Online]. Available: https://tools.ietf.org/html/rfc791 [Accessed: May. 12, 2019].
[5] "Internet of things" (IoT), "Wikipedia". [Online]. Available: https://en.wikipedia.org/wiki/Internet_of_things [Accessed: Feb. 22, 2019].
[6] R.Vinodkumar, S.Vijayalakshmi, K.R.Kavitha, K.Karthick, " Implementation of IPv6 Internet Service with MPLS Networks and MPLSL3VPN Service in IPv6 Networks," in International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-8 Issue-3, 2019. [Accessed: Dec. 22, 2019].
[7] About GEANT [Online]. Available: https://www.geant.org/About [Accessed: Feb. 22, 2019].
[8] [About MIXP [Online]. Available: http://www.mixp.me/ [Accessed: Feb. 22, 2019].
[9] RFC 2373 – IP Version 6 Addressing Architecture. [Online]. Available: https://tools.ietf.org/html/rfc2373 [Accessed: Feb. 20, 2019].
[10] RFC 3041 - Privacy Extensions for Stateless Address Autoconfiguration in IPv6. [Online]. Available: https://tools.ietf.org/html/rfc3041 [Accessed: Feb. 16, 2019].
[11] NAT64 Technology: "Connecting IPv6 and IPv4 Networks, CISCO". [Online]. Available: https://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/enterprise-ipv6-solution/white_paper_c11-676278.html [Accessed: Feb. 12, 2019].
[12] D. Gordon, I. Haddad, "Building a Linux IPv6 DNS Server". Open Systems Lab – Ericsson Research Corporate Unit. [Online]. Available: http://www.cu.ipv6tf.org/pdf/dns_v6.pdf [Accessed: Feb. 12, 2019].
[13] Postfix IPv6 Support. [Online]. Available: http://www.postfix.org/IPV6_README.html [Accessed: Jan. 12, 2021].
[14] RIPE Atlas measurement, [Online]. Available: https://atlas.ripe.net/measurements/28629350 [Accessed: Jan. 18, 2021].