ANALYSIS OF THE CAPABILITIES OF MPLS TECHNOLOGY FOR MANAGING TRAFFIC IN COMMUNICATION NETWORKS

DOI: 10.36724/2072-8735-2022-16-5-63-68

Manuscript received 20 April 2022;
Accepted 18 May 2022

Irina V. Stepanova,
MTUCI, Moscow, Russia, ***w515iv@mail.ru***

Knaj Nouma,
MTUCI, Moscow, Russia,
knajnouma@gmail.com

Keywords: *MPLS, VPN, Label Switching Technology, Multi Protocol label Switching, Virtual Private Network, QoS based on MPLS, MPLS Traffic Engineering, MPLS Tunnel*

To support a growing number of users and multiple classes of applications with different performance requirements and characteristics, service providers have been forced to adapt to new technologies. To improve traffic management and Internet service quality, the Internet Engineering Task Force (IETF) proposed MPLS technology to support several classes of latency-critical applications. Traditional IP networks use a hop-by-pop principle for transmitting traffic. This leads to aggregation of heterogeneous traffic on links in different parts of the network, which causes considerable possible growth of congestion and leaves the network with both unbalanced use of resources and link failure in congested parts. This raises the need for traffic engineering to ensure bandwidth guarantees and efficient use of network resources. To overcome these problems, the IETF has proposed a new data transmission mechanism, which is MPLS (Multi protocol label switching), in accordance with the current requirements. The application of MPLS (Multi protocol label switching) technology in modern communication networks is defined by the author as a research task. The report discusses the prospects of MPLS as a universal technology that supports several protocols. The features of construction of virtual private networks (VPN) on MPLS are considered, and how traffic engineering in MPLS takes into account the use of resources, which makes the development of routes based on separate streams or different streams between the same endpoints more effective.

Information about authors:

Irina V. Stepanova, *Associate Professor, Lecturer of the Department of Communication Network and Switching Systems, Ph.D. MTUCI, Moscow, Russia*

Knaj Nouma, *Student MTUCI, Moscow, Russia*

Для цитирования:
Степанова И.В., Кнаж Нума. Особенности организации сетей связи с привлечением технологии MPLS // T-Comm: Телекоммуникации и транспорт. 2022. Том 16. №5. С. 63-68.

For citation:
Stepanova I.V., Knaj Nouma (2022). Analysis of the capabilities of MPLS technology for managing traffic in communication networks. *T-Comm*, vol. 16, no.5, pp. 63-68. (*in Russian*)

In conventional IP networks, routing is based on the destination address and one parameter, such as the number of hops or the value of the delay. The router looks for the next hop (the closest) to the destination without taking into account the results of congestion control, this results the route closest to the destination to become the most congested.

There is another problem related to the characteristics of different packets, for example, voice and video packets are different in length and size and should have a higher priority than regular data packets. In addition, searching the routing table takes time, so packets carrying voice and video may not be able to reach their destination in order and time, getting stuck behind regular data packets. For these reasons, researchers have found that conventional IP packet forwarding is not suitable for applications such as VOIP and video conferencing, which are currently in huge demand.

This raises the need for traffic engineering to ensure bandwidth guarantees and efficient use of network resources.

To overcome these problems, the IETF has proposed a new data transmission mechanism, which is MPLS (Multi protocol label switching), in accordance with the current requirements.

MPLS is an extremely fast and efficient packet forwarding technology using labels look-up.

1. MPLS General Provisions

Each incoming packet in the MPLS domain is assigned a specific label depending on the destination address. An MPLS network consists of several routers called LSRs (Label Switching Routers), other routers that connect to IP routers are called LERs (Label Edge Routers).

An ingress router is a router within an MPLS domain, connected to the outside world, through which a packet enters the MPLS domain. The Egress Router is the router through which packets leave the MPLS domain. Each incoming packet is assigned a label, this label determines the most efficient and fastest label switching path (LSP) to direct traffic to the MPLS domain the entire way instead of finding the destination address at each point.

The concept of label switching is not new; it was developed from CISCO label switching.

Multiprotocol label switching is called a 2.5-layer protocol because it sits somewhere between layer 2 (the data link layer) and layer 3 (the network layer).

MPLS was provided as a high-value WAN connection from the service provider and applied to all other types of WAN also has another application as MPLS VPN.

2. MPL architecture

The MPLS architecture is divided into two components as shown in Figure 1.

1. orwarding Components: performs the forwarding of data packets based on the label that the packet carries.

2. ontrol components: used to create and maintain label forwarding information between groups of interconnected label switching routers. Used in measurements to implement simple load balancing techniques as dynamic traffic management to optimize network performance.

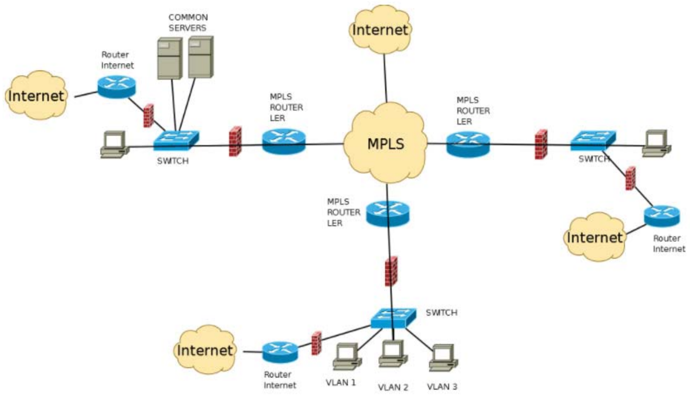

Fig. 1. MPLS architecture

MPLS technology supports the interconnection of many different technologies including IP routers, ATM switches and Frame Relay, as LERs support the connection of multiple ports as edge carriers in an access network.

At the edge router (ingress) a label is assigned to each incoming packet. These labels are distributed by the signaling protocol to create an LSP and forward traffic into the MPLS network.

The label switched routers are the main routers in the MPLS domain and are commonly referred to as core network routers.

When a packet enters the MPLS network, a label or labels are attached to it, and when these packets leave the MPLS network, these labels are removed by the edge routers.

2.1. MPLS header

The ingress router creates a small MPLS header 32 bits long to encapsulate each incoming packet (Fig. 2).

This little header is embedded between the level 2 and level 3 headers, which is why it's called a wrapper.

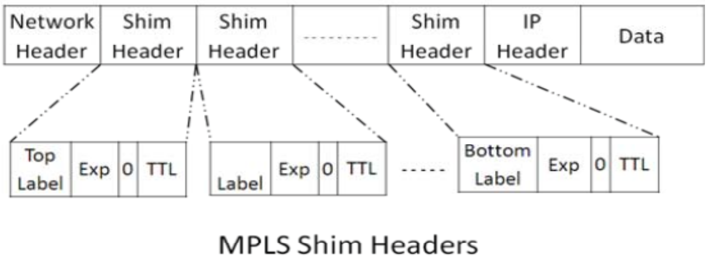

Fig. 2. MPLS Header

Top Label consists of 20 bits, which means it can have (2^20) values or labels.

(EXP) or experimental consists of three bits and is used for QOS-related functions. It is now renamed TF traffic class.

The next field is a single bit called bottom-of-stack. It is used as a flag when more than one label is assigned to a packet as in the case of the MPLS VPN or MPLS TE.

The next byte, the MPLS TTL (time to live) field, consisting of eight bits that can have a value from 0 to 255, serves the same purpose as the IP TTL byte in the IP header. Therefore, each time an LSR forwards a packet, it decrements the TTL field in the packet header, and if the value reaches zero the packet is discarded.

2.2. MPLS Label

An edge router and a label-switched router create a short, fixed-length object to decide where and how to forward the frame, this object is called a label (Fig. 3). All label information is specified in the Label Forwarding Information Base (LFIB).

L2 Header	Last Label	….	First Label	L3 Header

Fig. 3. MPLS label structure between Layer 2 and Layer 3 headers

At each LSR the old label is removed and a new label is inserted into the packet, and then the packet is forwarded to the next hop.

2.3. Using Forwarding Equivalence Class (FEC)

Forwarding Equivalence Class (FEC) is a group of packets that have the same characteristics and transport requirements.

All packets that have the same FEC are forwarded along the same path with the same processing. The function of assigning FEC to a packet is a function of the edge router as it is part of the MPLS domain, then all information is embedded in the label and attached to the packet. This way there is no more header analysis within the MPLS domain in the forwarding process.

3. MPLS Technology Features

3.1. Connection-Oriented TE and QoS support

There are some applications that require a high level of QoS, such as audio/video conferencing and VPNs. These High revenue-generating applications have always been the main focus of service providers.

The traditional conventional IP network cannot provide the necessary bandwidth for specific applications, and cannot provide an adequate level of QoS due to lack of support for traffic engineering, but is limited in scalability or flexibility, or sometimes both.

The Internet and service providers pose a new challenge due to some real-time or mission-critical applications because these applications have different latency, bandwidth, jitter and packet loss needs. On the Internet we have an unpredictable traffic flow, so there is a huge need for traffic engineering to run these applications efficiently.

IP (Internet Protocol) was not designed to support QoS, rather it was designed for education and research, but the network has to carry a large volume of traffic and still has limited resources, so it is important to allocate and optimize available resources. Allocating or scheduling network resources based on the required QoS to optimize the use of our network resources is known as traffic engineering.

In traditional IP networks, some links are congested, but others remain underutilized because of the destination-based forwarding paradigm.

Making a forwarding decision without considering the available bandwidth and traffic flow between the destination and the source will create congestion on that link, while leaving other links in the network unused, resulting in reduced bandwidth, latency and packet loss.

MPLS provides a solution by providing a connection-oriented structure on top of the current IP-based network to maintain the required level of QoS for these applications.

Traffic engineering in MPLS considers resource utilization, making it more efficient to design routes based on single flows or different flows between the same endpoints.

3.2. Multiple protocol support

There are two main planes in the MPLS architecture:

1-the control plane;

2-the data plane.

Control Plane: Performs information exchange between neighboring devices using various protocols such as OSPF (open Shortest Path First), IGRP (Interior Gateway Routing Protocol), EIGRP (Enhanced Interior Gateway Routing Protocol), IS-IS (Intermediate System-to-Intermediate System), RIP (Routing Information Protocol) and BGP (Border Gateway Protocol). Label exchange also takes place using TDP (Tag Distribution protocol), LDP (Label distribution Protocol), BGP, and RSVP (Resource Reservation Protocol).

Data plane: is based on labels and regardless of the routing protocol or label switching protocol, it simply forwards the packet. A label is assigned to each packet by searching the label forwarding information base (FIB) table, all information in the table is populated with TDP (label distribution protocol) or LDP (label distribution protocol).

From the name MPLS "Multi Protocol Label Switching" shows that MPLS has the wonderful feature of supporting multiple protocols.

The main advantage of MPLS is that it can be used with other networking technologies, as well as in pure IP, ATM and Frame Relay networks or even all three technologies, because a router that supports MPLS can coexist with a pure IP network as well as with ATM and Frame Relay switches.

Support for multiple protocols makes MPLS universal, which attracts other users with mixed or different network technologies.

4. MPLS operation method

LSP (label switched path) is a path through the intermediate LSRs from the entry and exit nodes in the MPLS domain (Fig. 4). All necessary information used to create the LSP is transmitted using two protocols between LSR.LSRs can transmit all packets depending on the label assigned to these packets.

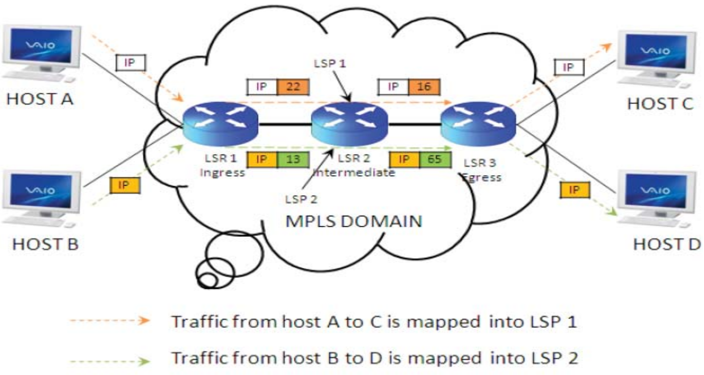

Fig. 4. A label-switched path on an MPLS-enabled network

One or more labels can be attached in the MPLS packet header, so here we do not have an IP table, but a label table, and packet switching uses label look-up instead of IP table look-up.

Adding a label to packets avoids route look-up to forward the packet over the LSP. To create an LSP, all labels must be distributed between MPLS nodes using the Label Distribution Protocol (LDP) or RSVP (Resource Reservation Protocol).

The flow of packets between the edge devices in the MPLS domain is defined by a label, which defines the forwarding equivalence class (FEC). Therefore, the packet forwarding process will take place along this label-switched route as virtual connections in a physical IP network without connection-oriented guaranteed processing (Fig. 5).

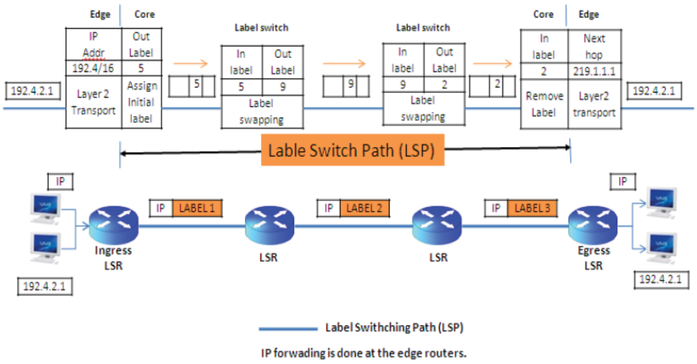

Fig. 5. Label assignment in the MPLS domain and IP forwarding

MPLS edge routers only can determine whether a packet belongs to a label and forward it by examining its header and their special database to allocate the destination address.

Forward Equivalence Class (FEC) is a class for identifying a group of packets that have the same characteristics, transportation, processing and routing requirements for the destination.

There are many parameters used to determine the FEC of a packet, such as source or destination IP address, source or destination port number, a DiffServ code point, and IP protocol identifier.

Each LSR builds a table called the LIB label information base, which is based on the FEC, the FEC is determined for each packet, then the corresponding label from the LIB is attached to it and it is forwarded through the LSP, each LSR checks and replaces the packet label with another corresponding label before sending the packet to the next nearest LSR to the destination via the LSP.

5. Virtua Private Network (VPN)

VPNs enable the use of the Internet as a transport medium, which means lower communications costs as well as the creation of local and isolated offices with secure links or enhanced communications between business partners.

With the MPLS edge model, there is no need to build a VPN using ATM (asynchronous mode transmission) or frame relays Permanent Virtual Circuits (PVCs).

MPLS VPNs can be implemented by adding an additional label to define the VPN and the corresponding VPN destination network, supporting an any-to-any communication model between offices or sites without having to install a complete PVC mesh along the provider's network, which helps simplify the process considerably compared to the PVC model as PVCs require routing management over a topological complex backbone.

The MPLS VPN differentiates the traffic services passing through the backbone into classes according to their QoS requirements.

6. MPLS Tunnel

In traditional IP routing, the routing decision is made on a hop-by-hop basis, comparing the needed destination address to the forwarding table.

In MPLS, IP routing information about all nodes on the way hop-by-hop to the destination is not necessarily, the decision based on the label carried by the received packet.

R4, R5, and R6 Service provider network, SW1 SW2 are customers (see Figure 6).

The goal is to transport packet between SW1 and SW2.

Case 1: traditional IP Forwarding:

AS100 runs OSPF on all internal interfaces, along with a full mesh of iBGP,

R4 is an EBGP peer with SW1, R6 is an EBGP peer with SW2.

We will assume that the layer two connectivity between the devices has already been established.

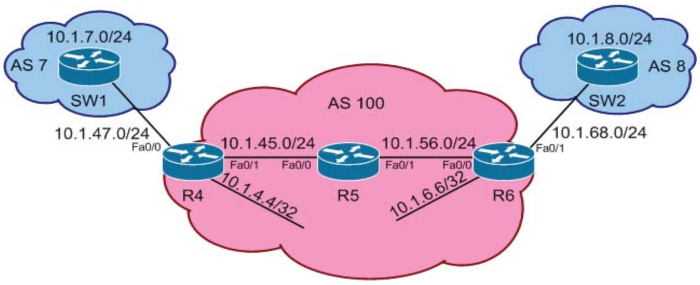

Fig. 6. MPLS Tunnel

The hop-by-hop traffic flow between AS7&AS8, from SW1 to SW2 then in reverse from SW2 to SW1, the verification should be done in both directions but the flow of packet from SW1 to SW2 is independent from SW2 to SW1.

SW1 learn via BGP about AS8 from R4 with a next-hop of 10.1.47.4. Packets going to 10.1.8.0 should be properly routed towards R4.

Next, the look-up process continues on R4:R4 learn via iBGP about AS8 from R6 with a next-hop value of 10.1.6.6.

R4 knows 10.1.6.6 via OSPF from R5, which uses interface FastEthernet0/1, packets towards 10.1.8.0 are now routed to R5, R5 learn via iBGP about AS8 from R6, with a next-hop of 10.1.56.6.

R5 should use interface FastEthernet0/1 to forward packets towards 10.1.8.0.

The look-up process now continues on R6: R6 learn via EBGP about AS8 from SW2, with a next-hop of 10.1.68.8.

R6 dictates that interface FastEthernet0/1 should be used to forward traffic to SW2.

SW2's look-up for 10.1.8.0 indicates that the destination is directly connected, and packets are routed to the final destination.

For return traffic back to AS7, a look-up occurs in the reverse direction, starting as SW2, and moving to R6, R5, R4, then finally to SW1.

In this hop-by-hop routing paradigm, in the transit path all devices must know routing information for all destinations they are forwarding towards.

If AS 100 was used for Internet transit, each router in the transit path would need +300,000 routes in their routing tables to provide transit to all Internet destinations.

With MPLS into this design, we can avoid the large routing tables in the core of the Service Provider network.

Case 2: MPLS Forwarding.

Enabling MPLS in the Service Provider network of AS 100, BGP can be disabled in the core, lightening the load on devices that are possibly already taxed for resource.

We'll look at the step-by-step process that occurs when an MPLS tunnel is functional in AS 100.

Enabling MPLS in AS100, allow us to disable BGP on R5, with additional BGP peering statements removed on R4 and R6.

R5 no longer has a route to AS7 or AS8 but it can still provide transit for traffic between them because MPLS tunnel has now been formed between the ingress and egress routers of the Service Provider network, which are R4 and R6 in this case.

SW1 looks up the route for AS8, and finds that it recurses to R4's next-hop value reachable via the fa0/0 interface, and the look-up now is R4 mission.

With BGP help, R4 finds the route to AS8 from R6 with a next-hop of 10.1.6.6. then R6 must find the outgoing interface to reach AS8.

The outgoing interface FastEthernet0/1 with a next-hop of 10.1.45.5.

In traditional IP forwarding, the packet need to be sent to encapsulate in the interface Fa0/1.

The interface fa0/1 is running MPLS so R4 should use the outgoing label value of 17 for 10.1.6.6/32, after searching in (LFIB) forwarding information base to know the assigned label to this interface.

In the LFIB, for 10.1.6.6/32 in the LFIB, the outgoing label value of 17 is used.

The label 17 will be added to the header of each packet is going to 10.1.8.0/24.

R5 receives the packet with an MPLS label number 17 in the header and he should look up in the MPLS LFIB first, not in the regular IP routing table.

In R5 LFIB, the local label 17 is associated with the destination 10.1.6.6/32, but the outgoing label to the final destination AS8 in no label.

R5 will remove MPLS label of 17 in a "POP" operation and forward it.

For packets from AS8 back to AS7, R6 adds the label 16 and forwards the packet to R5, then R5 removes the label 16 and forwards the packet to R4.

For any new routes from/to AS 7 or AS 8, AS 100 does not need to allocate new MPLS labels in Service Provider's core network. As long as MPLS transport is established between (R4 and R6) BGP peering address of the Provider Edge routers.

Traffic for any destinations can transit over the MPLS enabled Service Provider's core network without any additional forwarding information.

Conclusion

1) High revenue applications have always been the main focus of service providers. Internet and service providers have a new challenge because of some real-time or mission-critical applications, as these applications have different latency, bandwidth, jitter and packet loss needs.

2) On the Internet, we have unpredictable traffic flow, so there is a huge need for traffic engineering to run these applications efficiently. In traditional IP networks, some links are congested, but others remain underutilized because of the destination-based forwarding paradigm.

3) IP (Internet Protocol) was not designed to support quality of service QoS, rather it was designed for education and research, but the network must transmit a large volume of traffic and still has limited resources, so it is important to allocate and optimize available resources. Allocating or scheduling network resources based on the required QoS to optimize the use of our network resources is known as traffic engineering.

4) MPLS provides a solution by providing a connection-oriented structure on top of the current IP-based network to maintain the required level of QoS for these applications. Traffic engineering in MPLS considers resource utilization, making it more efficient to design routes based on individual flows or different flows between the same endpoints.

5) The main advantage of MPLS is that it can be used with other networking technologies, as well as with pure IP, ATM and Frame Relay networks, or even all three, since an MPLS-enabled router can coexist with a pure IP network as well as with ATM and Frame Relay switches.

6) MPLS tunnels similar to GRE and site-to-site IPSec VPN tunnels, transit traffic over devices without any knowledge of the traffic's final destination, MPLS tunnels use a combination of IGP, BGP learned information and MPLS labels.

References

1. S.N. Stepanov (2015). Teletraffic Theory: Concepts, Models, Applications. Moscow: Hot Line – Telecom, 868 p. (Theory and Practice of Infocommunications Series).

2. V. Olifer, N. Olifer (2018). Computer networks. Principles, technologies, protocols: Study book for universities. 5th edition. St. Petersburg: Peter. 992 p.

3. Vegeshna Srinivas (2003). Quality of service in IP networks. Fundamental principles of quality of service functions in Cisco networks: Translated from English. Moscow: Williams Publishing House. 368 c.

4. I.V. Stepanova, M.O.A. Abdulvasea (2017). Use of perspective technologies for development of the distributed corporate communication networks. *T-Comm*. Vol. 11, No. 6. C.10-15.

5. E.A. Kucheryaviy (2004). Traffic management and quality of service in the Internet. SPb: Nauka i tekhnika. 336 c.

ОСОБЕННОСТИ ОРГАНИЗАЦИИ СЕТЕЙ СВЯЗИ С ПРИВЛЕЧЕНИЕМ ТЕХНОЛОГИИ MPLS

Степанова Ирина Владимировна, *МТУСИ, Москва, Россия,* ***w515iv@mail.ru***
Кнаж Нума, *МТУСИ, Москва, Россия,* ***knajnouma@gmail.com***

Аннотация

В качестве исследовательской задачи автором определено применение технологии MPLS (Multi protocol label switching) в современных сетях связи. В статье обсуждаются возможности и перспективность MPLS как универсальной технологии, поддерживающей различные протоколы и обеспечивающей взаимодействие различных технологий без промежуточных преобразований. Рассматриваются особенности построения виртуальных частных сетей (VPN) на базе MPLS. Инженерия трафика в MPLS позволяет учесть использование имеющейся пропускной способности, что делает более эффективной разработку маршрутов на основе отдельных потоков или формирование различных потоков между одними и теми же конечными точками. Туннели технологии MPLS аналогичны туннелям технологий GRE и IPSec VPN вида "сеть-сеть" – трафик передается через устройства без каких-либо сведений о конечном пункте назначения. В туннелях MPLS используется комбинация IGP, полученной информации BGP и меток MPLS.

Ключевые слова: *MPLS, VPN, Label Switching Technology, Multi Protocol label Switching, Virtual Private Network, QoS based on MPLS, MPLS Traffic Engineering*

Литература

1. *Степанов С.Н.* Теория телетрафика: концепции, модели, приложения. М.: Горячая линия – Телеком, 2015. 868 с. (Серия "Теория и практика инфокоммуникаций").

2. *Олифер В., Олифер Н.* Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. 5-е издание. СПб.: Питер, 2018. 992 с.

3. *Шринивас Вегешна.* Качество обслуживания в сетях IP. Основополагающие принципы реализации функций качества обслуживания в сетях Cisco.: Пер. с англ. М.: Издательский дом "Вильямс", 2003. 368 с.

4. *Степанова И.В., Абдулвасеа М.О.А.* Использование перспективных технологий для развития распределенных корпоративных сетей связи // T-Comm. Телекоммуникации и транспорт, 2017. Том 11, №6. С.10-15.

5. *Кучерявый Е.А.* Управление трафиком и качество обслуживания в сети Интернет. СПб.: Наука и техника, 2004. 336 с.

Информация об авторах:
Степанова Ирина Владимировна, *доцент, преподаватель кафедрыССиСК, , к.т.н., МТУСИ, Москва, Россия*
Кнаж Нума, *студентка МТУСИ, группа М62002, Москва, Россия*