STVARANJE KVALITETNE MREŽNE INFRASTRUKTURE U CILJU USPJEŠNOG POSLOVANJA

CREATING A QUALITY NETWORK INFRASTRUCTURE FOR THE PURPOSE OF SUCCESSFUL BUSINESS

Muharem Redžibašić

Politehnički fakultet
Univerziteta u Zenici,
Fakultetska 3, Zenica

Ključne riječi:
mrežna infrastruktura, informacijska sigurnost, mrežna oprema, kolizijska domena, sigurnosni rizici

Keywords:
network infrastructure, information security, network equipment, collision domain, security risk

Paper received:
02. 12. 2021.
Paper accepted:
31. 12. 2021.

Stručni članak

REZIME

Brzim razvojem tehnologije mnogi poslovni procesi preneseni su na elektroničku obradu podataka, što je podrazumijevalo i razvoj lokalnih mreža u mnogim firmama i organizacijama. Većina mrežnih infrastruktura razvijala se inkrementalno, proširivala se prema potrebama i u većini slučajeva to je bio ad-hoc *pristup, bez puno planiranja i brige o sigurnosti. Mrežni implementatori uglavnom nisu bili stručnjaci, tako da su česti problemi na mreži i sigurnosni rizici. Mnoge današnje mrežne infrastrukture imaju zastarjelu mrežnu opremu koja je konfigurirana na protokole koji su postali još nesigurniji, a fizička implementacija mreže je često jedna velika kolizijska domena. Ovaj rad će predstaviti pristup, tj. kako se može kreirati kvalitetna mrežna infrastruktura i koji su ključni koraci u identificiranju slabih tačaka mrežne infrastrukture.*

Professional paper

SUMMARY

The rapid development of technology caused many business processes to start using electronic processing of data, what implied development of local networks in many companies and organizations. Most network infrastructures have been developed incrementally, and expanded according to the needs, and mostly an ad-hoc approach was applied, without a lot of planning and taking care of security. Network implementers, in general, were no professionals, so the network issues and security risks happen often. Many pieces of today's network infrastructure have obsolete network equipment, with configured protocols that have become insecure, and physical implementation of the network is often a big collision domain. This paper will present approach, i.e., how a quality network infrastructure can be created and what are the key steps in identifying the weak points of the network infrastructure.

1. NETWORK INFRASTRUCTURE

A computer network can be viewed as a communication system, where information generated on the one side is delivered to the other. This paper mainly deals with local area networks (LANs) that the most users use in their homes, companies, or institutions.

The definition that will be singled out according to the Croatian Academic and Research Network (CARNET) says: "A computer network consists of a group of interconnected computers. Networks can be classified according to size, connectivity, functional connection, and architecture." [1].

LANs are used to connect computers and other network devices to share resources (such as printers) and exchange information over a network [9].

The implementation of each network must go through certain stages, which are most often: *network design phase, network implementation phase, network documentation, etc.* Each network is a system that consists of certain parts and that develops over time. The question is when it can be said that the network implementation process is complete. The answer is never. The network goes through constant modifications and expansions in its lifetime, and every change needs to be monitored through these phases, so it is very important to follow new trends in technology and networks to be able to identify shortcomings and improve the network. It is very important if it can be managed to prevent some things in due time, before setting everything up again.

1.1 Design phase

When designing LANs for medium and large companies, it is best to use a three-layer hierarchical model. The hierarchical model involves dividing the network into discrete layers. Each layer provides specific functions that define its role in the entire network. This achieves a modular design that ultimately results in better performance and greater network scalability. The three layers that make the hierarchical network model are:

1. Access layer,
2. Distribution layer, and
3. Core layer.

Applying this model brings many advantages, such as, first, **network scalability**, which refers to the possibility of simple system scalability. According to Figure 1, it is enough to add a switch device, connect it to the distribution layer and our network is simply expandable - scalable.
Redundancy - this feature is important, especially when there is a network that provides services for the so-called 'mission critical' applications, where connectivity is imperative. Redundant links provide alternative links to the destination, making the network resistant to sudden falls of parts of the network.
Security - a three-tier hierarchical model allows users to create specific security policies on each of these layers. Security can be implemented at the level of ports, virtual LANs, access lists, etc.
Manageability - such networks are easier to manage. The necessary interventions can be done and focused on individual parts or at the level of a particular layer, without affecting the rest of the system.

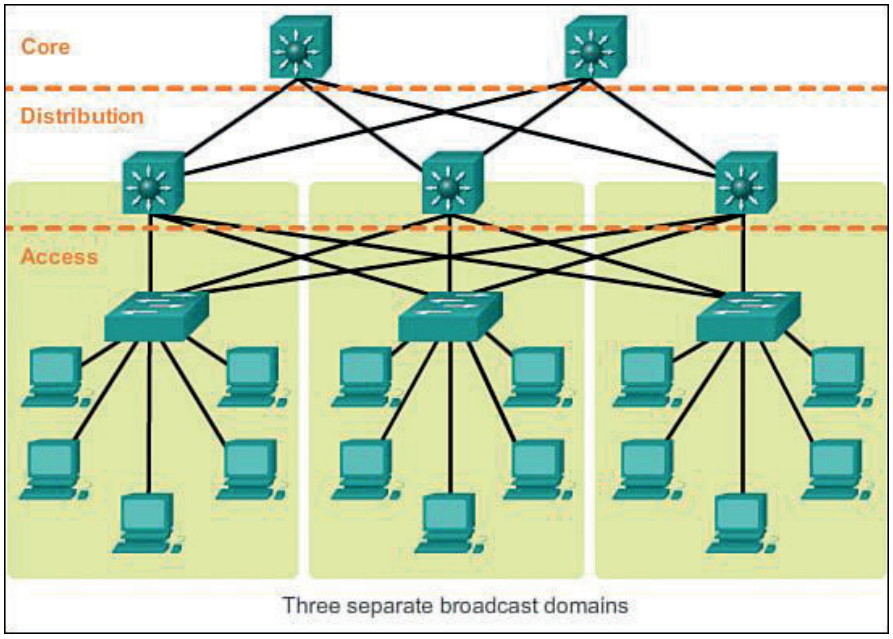

Figure 1 *Hierarchical network model [3]*

If the computer network is designed as a new one, then definitely this model is important. However, in the case of reconstructing the existing network, it is needed to make as many changes as possible to bring the existing situation closer to this hierarchical model, solely for the advantages mentioned above.
It is very important to mention that the network documentation is a document that is created at the time of network design, supplemented by elements related to implementation[1], containing information about a particular class of administration, and other pieces of information related to network functionality. Depending on the size of the network, paper can be used or some programs with automatic support for tables, and if the network is more complex, there are even specialized software solutions. Therefore, any data related to operating and functioning of the network should be part of the

[1] Implementation is the phase when works are performed in order to implement the network defined in the project. It includes laying cables, mounting connectors and connecting to patch panels, marking cables and sockets, implementing cable guides and channels, grounding, etc.

network documentation. Documentation is a document that is developed and maintained over the life of the network. If the documentation is not up to date, it can represent a bigger problem than if it's not present at all, because it can lead a user to wrong conclusions.

1.2 Structural cabling

The emergence of a large number of different network equipment manufacturers has led to the need to define standards that would cover general aspects of networking. The set of standards related to networking is called structural cabling. Structural (generic) cabling includes all possible types of cabling.

The purpose of structured cabling is to introduce rules for planning and implementation of computer networks. As an example, structured cabling will be mentioned, which includes saturated cabling, that envisages the installation of two connections on every 2-3 m^2 of working space. This approach is used for networking in facilities where the exact layout of computers and other IT infrastructure is not known.

Structured cabling involves cross connections (distribution facilities) and patch panels (switchboards), all with the aim of ease restructuring the computer network.
The standards related to structured cabling are:

- ISO / IEC IS11801 - International standards
- EN 50173 - European standards
- EIA / TIA 568 - American standards

It is very important to note that when cabling adhere to one of the standards and respect all the elements of structured cabling, where special attention have to be payed to backbone cabling where this type of cabling is used to connect main distribution facilities (MDF) with intermedia distribution facilities (IDF). Backbone cabling should be performed using network media with as much bandwidth as possible (e.g., optical cables).

In order to improve the existing network infrastructure, an analysis of the state of the network is needed and, if there are resources, the bandwidth in relevant part of the network should be improved.

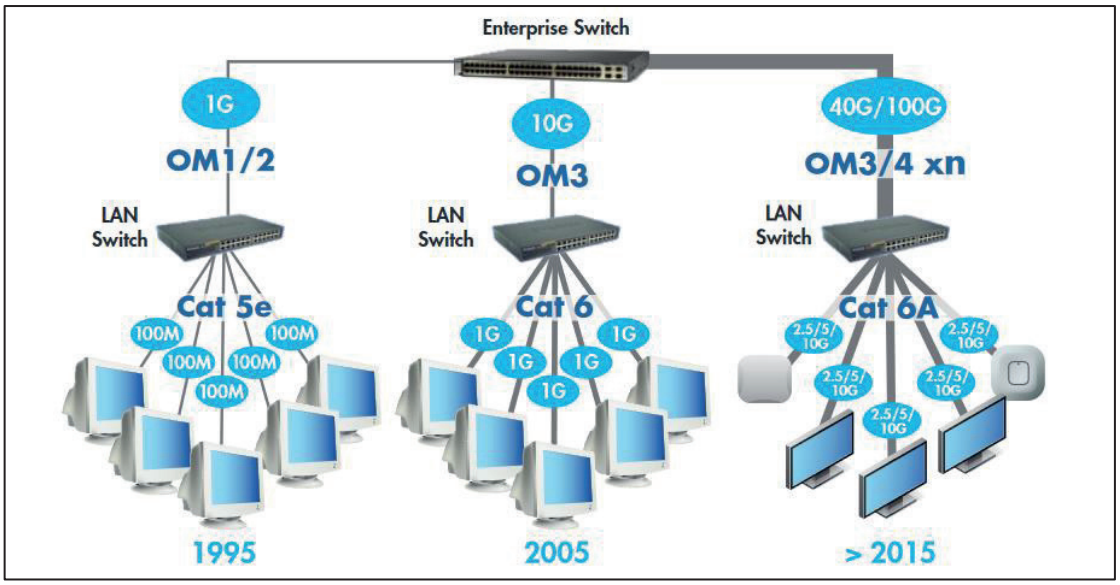

Figure 2 *LAN cabling [4]*

2. STEPS TO IMPROVE NETWORK INFRASTRUCTURE

This chapter will cover some of the key things to look out for when considering a network infrastructure, whether building a new one or reconstructing an existing one. The things covered in this chapter will actually be the key things to look out for in order to improve or identify vulnerabilities in a particular network infrastructure.

2.1. Collision domain

A collision domain is a shared network segment where a collision can occur, that is an area of the network that would be affected by a collision. Regarding the devices of the first layer (OSI reference model), due to the mode of action, signal amplification and its transmission, such devices increase the collision domain.

Second level of devices do segmentation (division) of the collision domain. The switch, on the other hand, does micro segmentation, where each port on the switch, and each device connected to the switch, represent a separate collision domain, and if it is a full duplex communication, then it is a collision-free environment, an environment without the possibility of collision. It is because the switch has almost eliminated the use of hubs in computer networks.

In practice, this would mean that wherever is a hub device, it is not a big investment to replace it, but in terms of the performance of our network, it will be very important.

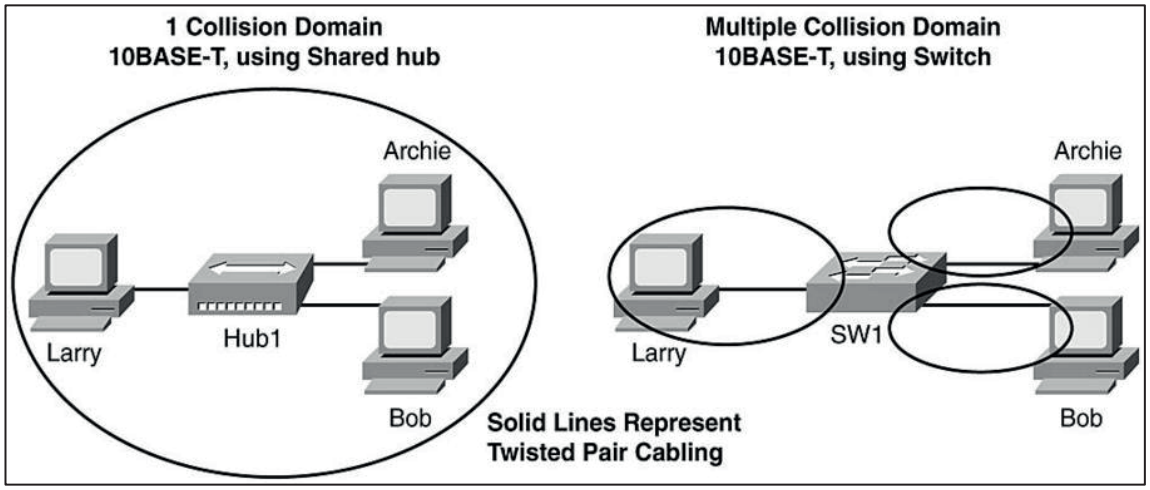

Figure 3 *Collision domains [2]*

2.2. IP addressing and subnets

An IP address allows to uniquely identify a host on a network. Without a proper addressing scheme, communication between computers would not be possible. To make address management easier, all addresses are divided into specific IP address classes. In the original Internet routing scheme developed in 1980, IPv4 addresses were divided into 5 classes. These are Class A, Class B, Class C, Class D and Class E. The last two classes are special purpose classes, and are less commonly used.

Mostly, many institutions and organizations did the addressing poorly, with unnecessary loss of IP addresses. To avoid it, it is necessary to use subnets (subnetting).

When talking about subnetting, it means that one whole class (A, B, C) is divided into several small ones, thus minimizing the loss of IP addresses. The recognition of subnetting is by the fact that certain hosts are assigned to the network part. It can be best established whether a network is subnetted by the subnet mask. If the value of the subnet mask is different from the default one, then it can be said it is a subnetted network.

Subnetting allows an administrator to divide a particular network into several small ones to fulfil the task of addressing devices on the network.

If the network is divided into subnets, there are many benefits, such as:

- reducing network traffic,
- optimizing network performance,
- making it easier to spot and solve network problems, and
- increasing network security.

2.3. Updating firmware

Firmware is a program that is permanently installed on hardware devices such as routers. It is programmed to provide constant instructions for communicating with other devices and perform functions such as basic input / output tasks. The firmware is usually stored in the flash ROM (read-only memory) of the hardware device. It can be deleted and overwritten [5].

The firmware was originally designed for high-level software, and it can be replaced by a new device without replacing the hardware. The firmware, also, retains basic instructions for the hardware devices that make them operational. Without the firmware, the hardware device would be non-functional [7]. Flashing firmware update involves overwriting existing firmware or data, contained in EEPROM or flash memory modules present in the electronic device, with the new data. Some firmware cannot be overwritten, while others are upgradeable, meaning it is possible to upgrade the firmware of the device by connecting to a computer in a specific configuration and then run the software of the manufacturer.

This process is called 'flashing firmware' or simply 'flashing'. This becomes necessary when a device becomes incompatible with new operating systems, or simply when there is a need to improve device performance [8].

For example, for network devices such as routers and modems, it is very important to check on the official website of the manufacturer the latest version of the firmware available and compare it with the current version on the device. If a new version is available, there is a need to upgrade existing one. Before upgrading, it is always recommended to back up the existing firmware and device configuration, so if a problem occurs, it can be restored to its original state. Firmware upgrades are mainly performed to improve performance, but if it is a network device, then it is very important to do so for the sake of security. Often some devices with older firmware versions become vulnerable to certain malicious code types and to protect and prevent something unexpected from happening with big consequences on the network, a firmware update to the latest available secure version has to be done.

3. EXAMPLE

In this section, a typical network diagram, where the computer network was created incrementally, will be presented, and after that a reconstructed network diagram with suggestions for improvement will be presented, too.

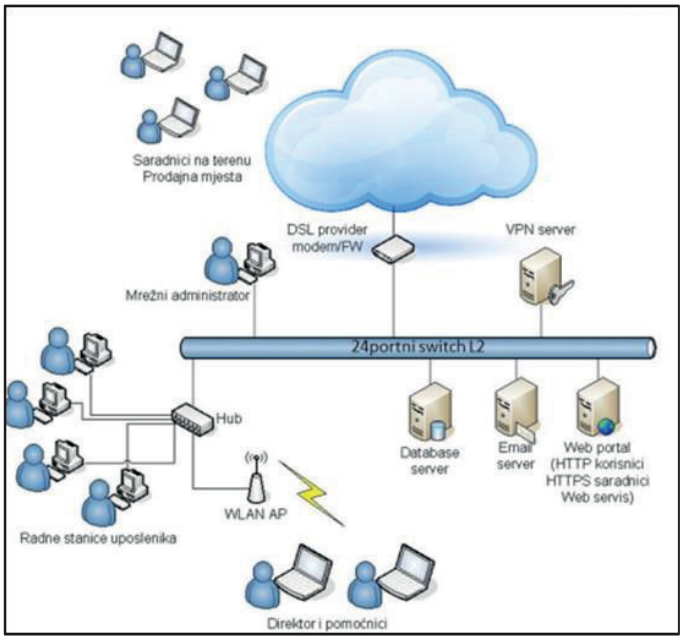

Figure 4 *Example of weak network infrastructure (Source: authors)*

A closer look at the previous picture shows many shortcomings. First, there is a hub device that expands the collision domain, and it is very slow. So, in order to reduce the potential number of collisions, there is a need to replace the hub device with a switch device, which will increase the number of collision domains, and reduce the number of potential collisions in the network and thus gain speed. Second, it should be noted that a DSL modem is used from a provider that is also a router. For a more professional approach, it is necessary to keep the device from the provider, but to use only the modem function, and for other services and settings to use other, more sophisticated, devices with more features and higher memory, such as a separate router. In this way, it can be achieved, in addition to security, a gain in performance, and as well, the scalability property prescribed by the hierarchical network model, described in the first chapter of this paper.

It is also clear that servers, employees, administrators and everyone else are on the same subnet. From the aspect of security, this is not satisfactory, and the suggestion is to set up a security network device (firewall) and to separate subnets according to the type of equipment and relevant users.

Also, regarding wireless access, there is only one wireless access point, what represents vulnerability, because they are all connected via the same access point. Since we need to separate different types of users into different subnets, a good move would be to install another wireless access point to serve only visitors / guests. This access will be separated from the internal network. Also, VLANs should be implemented for logical segmentation.

After all the above, an improved network infrastructure diagram can be presented.

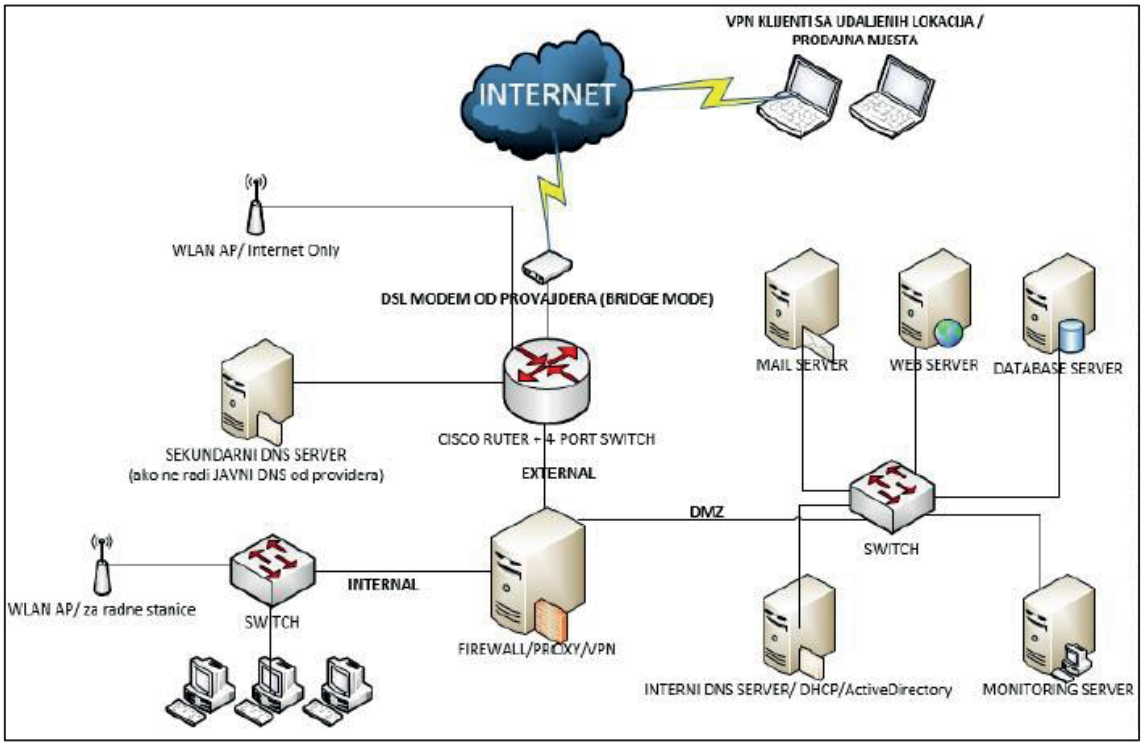

Figure 5 *Example of improved network infrastructure (Source: authors)*

4. CONCLUSION

Given that many of today's network infrastructures have outdated network equipment with physical network implementations that are quite poor, and they very often represent one major collision domain. From the very phase of network design, clearly a three-layer hierarchical model of network infrastructure should be adhered to. If it is possible to reconstruct the existing network infrastructure, there should be done things that will resort to the greatest degree to the hierarchical model of network infrastructure. Also, a great importance is put on the structured cabling, where is very important to do everything in accordance with the predefined

standards, and to make quality network documentation, in a way that any piece of information related to the operation and functioning of the network is a part of the network documentation.
For the smooth functioning of the computer network, it is very important to reduce the area of the network that could be affected by the collision. This can be achieved by increasing the number of collision domains, by replacing network devices and, thereby, reducing the area of the network that could be affected by the collision. Also, to optimize network performance and increase security, there is a need to do quality IP addressing in the network. One way to achieve these goals is to introduce subnets. The security can be increased by having adequate monitoring firmware versions on network devices and by updating them.

Malicious users and malicious types of program code can cause not only a financial damage, from which most entities recover, but can also cause life-threatening damage. *Killware* is a new term in cyber security that refers to the malicious use of information technology that can result in the loss of human lives. An example of such an attack was in Florida, USA, where a malicious user tried to contaminate water in a plant from which water is delivered to the population. Furthermore, failures in healthcare, where people depend on medical devices that are connected and controlled through a computer network and software, are inadmissible. The same case is with the car industry and the advent of autonomous vehicles where applying malicious code to such systems could greatly compromise human safety and lives.

Therefore, planning, designing, implementing and maintaining a computer network infrastructure is not a negligible process and a quality approach to it can be a prevention of many potential security risks, especially in an age when each device is more or less connected to some type of computer network [6].

This paper identified the key things related to creating a quality network infrastructure and it suggested steps that should be primary if the goal is to improve the existing network infrastructure and maintain a successful business.

6. LITERATURE

[1] CARNet - Croatian Academic and Research Network, (2009.), „Sigurnosni model mreže računala“, p. 6.
[2] CCIE Study Blog, „Ethernet: Collision Domains and Switch Buffering“, https://bethepacketsite.wordpress.com/2016/02/10/ethernet-collision-domains-and-switch-buffering (accessed 20.10.2021.)
[3] Cisco Networking Academy Connecting Networks Companion Guide: Hierarchical Network Design, http://www.ciscopress.com/articles/article.asp?p=2202410&seqNum=4, (accessed 19.10.2021.)
[4] COMMSCOPE White Paper, „Fiber Backbone Cabling in Buildings“ https://www.commscope.com/globalassets/digizuite/2506-fiber-backbone-in-buildings-wp-109423-en.pdf?r=1, p. 3., (accessed 21.10.2021)
[5] Halonja A., Milica M., (2009.) „Računalni nazivi sa elementom – WARE u engleskome i hrvatskome jeziku“, Rasprave Instituta za hrvatski jezik i jezikoslovlje, p. 116.
[6] Official PANDA Security Website, https://www.pandasecurity.com/en/mediacenter/security/what-is-killware/ (accessed 15.11.2021.)
[7] Official TACHOPEDIA Website, https://www.techopedia.com/definition/2137/firmware, (accessed 25.10.2021.)
[8] Official TECH-FAQ Website, „Flashing Firmware“, http://www.tech-faq.com/flashing-firmware.html, (accessed 25.10.2021.)
[9] Tanenbaum A., Wetherall D., (2013.) „Computer Networks“, Fifth edition, University of Washington , p. 19.

Corresponding author:
Muharem Redžibašić
Politehnički fakultet Univerziteta u Zenici,
Fakultetska 3, Zenica
Email: r.muharem@gmail.com
Phone: + 387 61 629 136