Emerging Research and Solutions in ICT 1(1):32–44 DOI: 10.20544/ERSICT.01.16.P04
UDC: 004.738.4.056:377.36.091.64

Modeling and evaluation of VPN laboratory exercises for Information Technology curricula

Dalibor Dobrilović [1], Željko Stojanov [1], Borislav Odadžić [1], Tamara Zoric [1], Danijel Žurma[2], and Žiga Petrič[2]

[1] University of Novi Sad / Technical Faculty "Mihajlo Pupin" - Zrenjanin
23000 Zrenjanin, Serbia
dalibor.dobrilovic@uns.ac.rs, zeljko.stojanov@uns.ac.rs,
odadzic@tfzr.rs, tamarazoric27@gmail.com
[2] Tehna d.o.o, Ljubljana, Slovenia,
1000 Ljubljana, Slovenia
ziga.petric@tehna.si, daniel.zurma@tehna.rs

Abstract. Establishment of a secure connection over Internet in industrial and commercial environments is very important. Considering that, information technology (IT) professionals are in charge for implementing the appropriate technologies. Therefore, the efficient IT security training inclusion in the university courses has the crucial role. The creation of VPN laboratory exercises for industrial Ethernet and business communication is presented in this paper. The VPN exercises are implemented on two laboratory sets for teaching VPN, the first one based on Allen-Bradley® communication equipment in combination with other hardware and software components, and the second platform based on Cisco routers. The qualitative study was conducted in order to analyze student's experiences. Research findings indicate the importance of students experience in using learning materials and scenarios, experience in problem solving and using laboratory sets for mastering VPN technology.

Keywords: VPN laboratory platform, VPN teaching scenarios, engineering education, students experiences, qualitative study

1. Introduction

The expansion and growth of information and communication technology (ICT) utilization in business and industry, and raising treats in data and system security make challenges for university engineering education and lead to ICT curricula changes. The university courses related to IT, in the field of Data and Networks security have to cover Virtual Private Networks (VPN) technology. VPN is not new technology, but its implementation in university curricula represents the constant challenge.

In this paper, an approach in modeling two laboratory sets for teaching VPN technologies is presented. The first laboratory set is based on industrial Allen-Bradley® Stratix5900 Service Router produced by Rockwell Automation, Inc [1]. Cisco Catalyst

2950 24 port switch, and Wireshark network analyzing tool are included in the laboratory equipment. The second laboratory set is based on Cisco routers with similar support of hardware and software. Together with hardware and software components of the platform, the scenarios for their usage are presented in this paper.

In order to explore some preliminary students' experiences with the platforms, a small scale qualitative empirical study was organized. The study was based on collecting students' opinions by using interviews and analyzing the transcripts by using general inductive approach [11]. The findings are presented as a framework with categories related to different types of experience gained in the laboratory.

This research is based on the initial research presented in [15], and represents its extension. The extension of the initial research presents the ongoing work directed towards improving the VPN lab exercises and evaluation of their implementation.

2. Platforms for the course

The challenging task of creating efficient lab sets for teaching VPN is tackled in this research with two approaches. Both approaches rely on laboratory platform sets supported with the network scenarios. The platform sets are based on equipment provided by two vendors. The description of both platform sets is given. The components of the platforms are presented in details, as well as the mode of their usage and the roles they have.

2.1. Allen-Bradley platform

The first platform for this lab exercise consists of seven components. Those components are presented in the Table 1.

Table 1. The components of the VPN lab based on Stratix routers

No.	Item	Description	Role
1	Allen-Bradley® Stratix 5900	Service router	Router A in the scenario
2	Allen-Bradley® Stratix 5900	Service router	Router B in the scenario
3	Cisco Catalyst 2950 24 port Switch	L2 switch	Public network
4	Computer A	Win 7 OS	PC and network on the side of Router A
5	Computer B	Win 7 OS	PC and network on the side of Router B. Network analyses station and configuration station for both routers.
6	Quick 'n Easy FTP Server 3.2	Software on computer B	Service provided to the users in order to demonstrate secure and unsecure connections
7	Wireshark	Network analyzing tool	Software tool for simulating network
8	Router configurator tool	Stratix 5900 Configuration tool	Installed on Computer A for configuring routers.

The network components are deployed as it was presented at Figure 1. The first two components are routers Allen-Bradley® Stratix 5900, representing one router connected to the core network of a company, and one router connected to the far branch of a company. Stratix 5900 is fully integrated with Cisco IOS. It has one wide area network (WAN) port and four additional Ethernet-ports. It supports: firewall capabilities, Virtual Private Network (VPN), intrusion protection capabilities, Network Address Translation (NAT), NBAR protocol filtering, Access Control Lists (ACL) and Quality of Service (QoS). [2]

Cisco Catalyst 2590 24 Switch is L2 switch (item 3 in Table 1), playing the role of the WAN or Internet public network with IP addresses from the pool 192.168.100.0/24. The capability of monitoring network traffic is crucial in this scenario [3].

Using the Cisco Catalyst 2950 SPAN (Switched Port Analyzer) feature, the switched segment and direct communication between two Stratix 5900 routers is forwarded to the port 22 of the switch – the monitoring port of the network, allowing all packets to be forwarded to the Computer A (USB Ethernet adapter) in order to be analyzed with the Wireshark network analyses tool. Wireshark [4, 5] is the world's most widely used network protocol analyzer. It lets IT experts to explore what is happening on the network at a microscopic level. It is de facto (and often de jure) standard across many industries and educational institutions.

Wireshark (item no. 7 in Table I) has a rich feature set including the following: deep inspection of hundreds of protocols, live capture and offline packet analysis, standard three-pane packet browser, multi-platform support (runs on Windows, Linux, OS X, Solaris, FreeBSD, NetBSD, and many others), captured network data can be browsed via a GUI, or via the TTY-mode TShark utility, rich VoIP analysis, etc. The Wireshark read/write many different capture file formats: tcpdump (libpcap), Pcap NG, Microsoft Network Monitor, and many others. Output can be exported to XML, PostScript®, CSV, or plain text.

The Computer A (item no. 4 in Table I) is presented with two images. The computer with IP address 172.16.200.2 and the computer with the IP address 10.10.10.2.

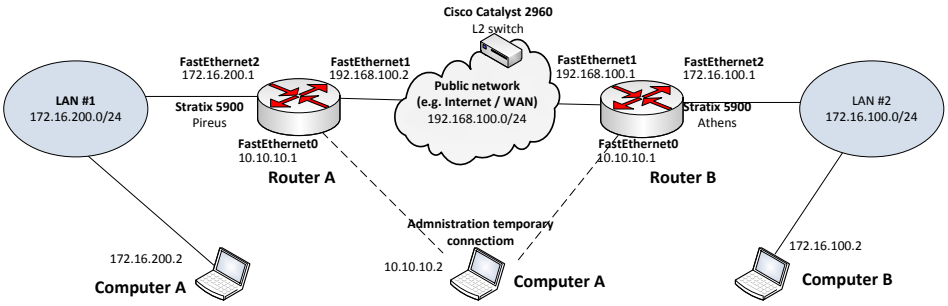

Fig. 1 Laboratory components for VPN lab based on Stratix

Basically, this is the same physical machine – laptop, with one network interface, and one additional USB adapter network interface. This configuration allows two LAN Ethernet connections at the same time. One interface is used for playing the role of Computer A in the scenario with IP address 172.16.200.2. Other interface is used to configure either Stratix 5900 router A or Stratix 5900 router B. This network interface is

with network address 10.10.10.2, or any other address from the pool 10.10.10.0/24 except 10.10.10.1.

Computer B (item no. 5) plays the role of a computer placed in the branch office, on the far side of the network. It has installed FTP server for providing connectivity and data transfer, and for demonstrating to the students difference between encrypted and unencrypted traffic. The installed version of the FTP server is Quick 'n Easy FTP Server 3.2 (item no. 6). Its purpose is to enable lecturer to open one user account in order to provide access to FTP server on Computer B from Computer A and to provide data transfer.

The Stratix Configurator is program provided by the Allen-Bradley® for configuring Stratix routers. It is a program developed in Java. It requires Java runtime machine for execution, and allows easy and menu guided installation. This program will be used in the lab exercise for setting up and establishing a VPN connection.

2.2. Cisco platform

The second platform set is based on Cisco routers. The components of this lab set are given in Table 2. The difference in hardware is minor, while the differences in scenario are significant. The main difference in this VPN scenario is utilization of three instead of two routers.

The third router plays the role of Internet. The reasons why the third router is introduced in this scenario are as follows: the number of available Cisco routers is bigger than number of Stratix routers, idea to make VPN scenario more complex for configuration, and finally to make this scenario more descriptive in order to present VPN systems in the broader sense.

Table 2. The components of the VPN lab based on Cisco routers

No.	Item	Description	Role
1	Cisco 1921 router	Router	Router A in the scenario
2	Cisco 1921 router	Router	Router B in the scenario
3	Cisco 2901 router	Router	Router C in the scenario
4	Cisco Catalyst 2950 24 Switch	L2 switch	Public network
5	Computer A	Win 7 OS	PC and network on the side of Router A
6	Computer B	Win 7 OS	PC and network on the side of Router B. Network analyses station and configuration station for both routers.
7	Quick 'n Easy FTP Server 3.2	Software on computer B	Service provided to the users in order to demonstrate secure and unsecure connections
8	Wireshark	Network analyzing tool	Software tool for simulating network
9	Putty	Terminal software	Installed on Computer A and B for configuring routers.

Other components have the same role as in the first scenario. The second difference between two scenarios is in usage of putty – a terminal program used for configuring of Cisco router with standard CLI Cisco IOS commands. The Computer B used for configuration is connected to the router console port using USB to Serial adapter and

console cable. All three routers can be configured with one set of USB to Serial adapter and console cable, or they can be connected separately with multiple adapter/cable sets. The second variant is used in the exercise.

3. VPN scenarios

VPN scenario used in this lab exercises is simple site-to-site VPN (Fig. 2). It should represent the simple way to securely connect two sites [6]. On one side is company HQ and on the other side is remote branch office.

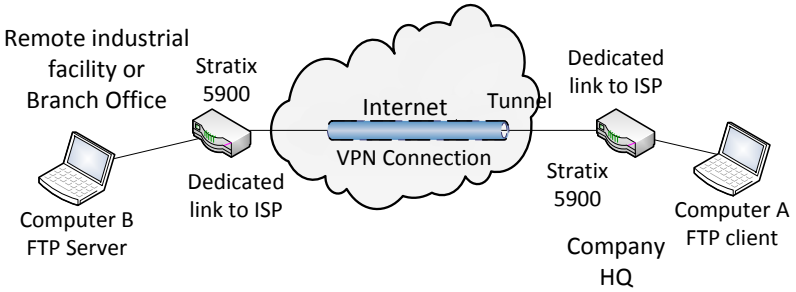

Fig. 2 Simple site-to-site VPN scenario

The first part of the scenario includes establishment of simple network connectivity without encrypted tunnel. The simple IP addressing and static routing is configured on Stratix 5900 service routers in the first lab exercise and on the Cisco routers in the second one. In the second scenario, the third router is placed in the center of the network representing the Internet. The configuration of IP addresses was made with web configuration interface and web browser in the Stratix 5900 case. The exact steps for this configuration will be shown in the next section.

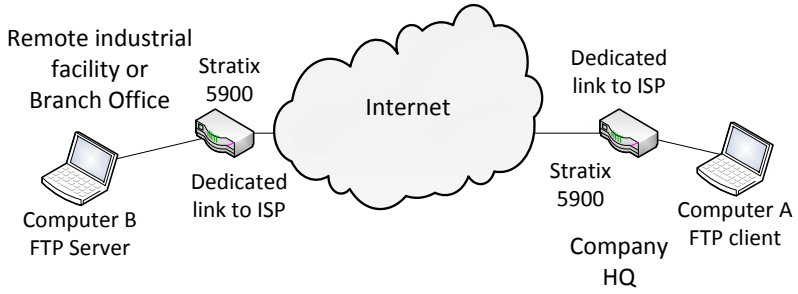

Fig. 3 Network connectivity without encryption

The configuration of Cisco routers is made in more classical way; with terminal software named putty, and using standard Command Line Interface (CLI) commands. The non-encrypted scenario is presented in Fig. 3.

4. Routers configurations in scenarios

The configurations of routers in both scenarios are presented in this section. The configuration of the Stratix routers is presented in more details, since the Stratix are less presented in the market, and represents something new introduced in university courses. The configuration of the Cisco routers is only descriptive without details, because it is widely know platform.

4.1. IP addressing and static routing of Stratix routers

As it was told before, the first step in configuration of a non-encrypted connection is accessing the routers and configuring their IP addresses. In order to configure routers, the interface card on the Computer A should have assigned IP address 10.10.10.2. The connection to the router can be made with the browser using IP address 10.10.10.1. The access to the router's web interface and its options are presented in Fig. 4.

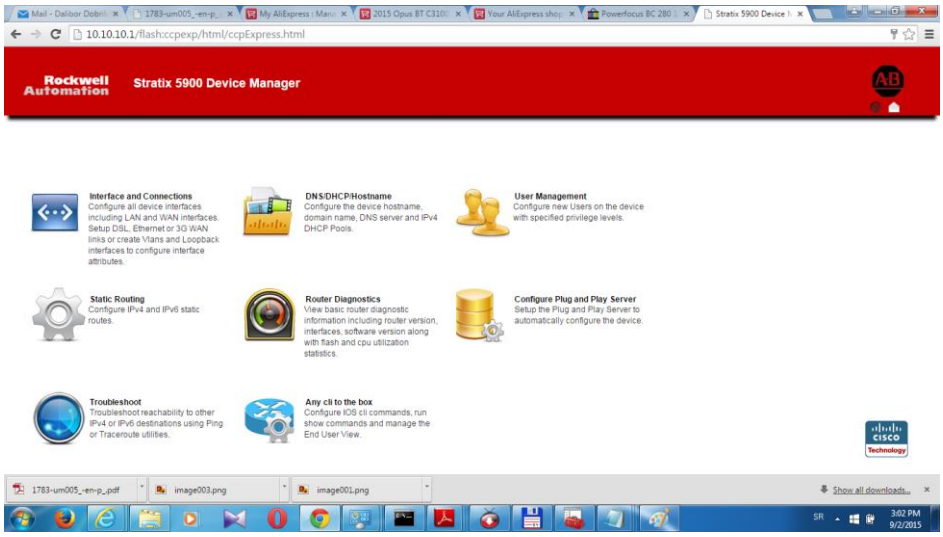

Fig. 4 Web interface of Stratix 5900 service router

The IP address interface setting for Router B is made by creation of two additional VLAN's - VLAN2 and VLAN3 besides existing VLAN1. The VLAN1 with address 10.10.10.1 stays associated with FastEthernet0 interface of Stratix 5900, VLAN2 with IP address 192.168.100.1/24 should be associated with FastEthernet1 interface, and VLAN3 interface (172.16.100.1/24) with FastEthernet2.

The similar settings are for the second router (Router A). VLAN1 has IP address 10.10.10.1 and it is associated to FastEtherent0 interface, VLAN2 (192.168.100.2/24) to FastEthernet2 and VLAN3 (172.16.200.1/24) to FastEthernet3 interface. The listing of interfaces is given on the Fig. 5 after successful configuration.

The next step in configuring routers is addition of one static route to each router. This route may be added as a default route (0.0.0.0/0) to the gateway - FastEthernet1 interface on the router of the opposite side, or the route to the network on the opposite side of connection – e.g. route to the network 172.16.100.0/24 on the Stratix 5900 router A via FastEthernet1 interface of Stratix 5900 router B with IP address 192.168.100.1. On the router B the added route can be route 172.16.200.0/24 via gateway 192/168/100.2.

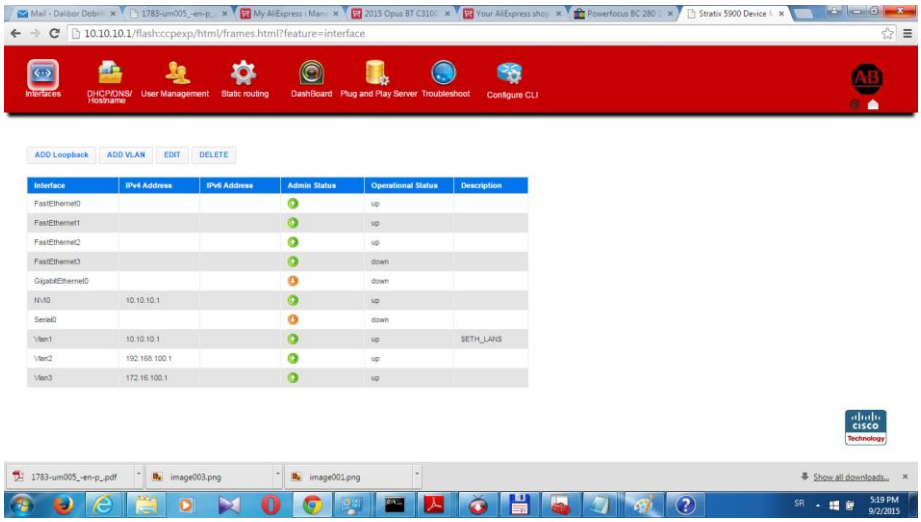

Fig. 5 Interface configuration of Stratix 5900 service router A

4.2. Establishing site-to-site VPN connection with Stratix routers

The establishment of secure VPN connection for this purpose is made with Stratix Configurator. The configuration details are presented in Fig. 6. The set of menu options which lead to the screen on Fig. 6 are *VPN* > *Site-to-site VPN* > *Create site-to-site VPN* > *Quick setup*.

The major parameters, which should be taken into account are as follows. The selected interface should be VLAN2 for both routers. Select type of peers should be Peer with static IP addresses for both routers. Address of the remote peer should be 192.168.100.1 on router A, and 192.168.100.2 on router B. Pre shared key should be made by choice and to be the same for each router. The traffic to encrypt parameters should be VLAN3 for source, and 172.16.100.0/255.255.255.0 for destination on router A, and VLAN3 for source, and 172.16.200.0/255.255.255.0 for destination on router B.

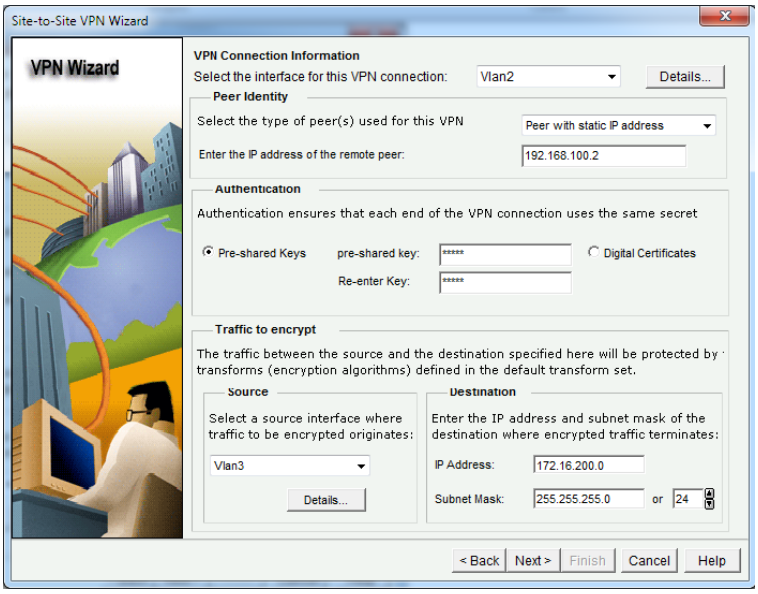

Fig. 6 Creation of site-to-site VPN on Stratix 5900 service router A

4.3. The configuration of Cisco router for second scenario

The configuration of a Cisco scenario will not be given in details. The reason is that Cisco routers are widely used for a long period, so the configuration of those routers is well known to experts and students. The configuration is made in two steps like in previous scenarios. The first step is IP addressing and configuring dynamic routing. The dynamic routing protocol used in this scenario is EIGRP. The IP addressing and EIGRP routing are made on all three routers.

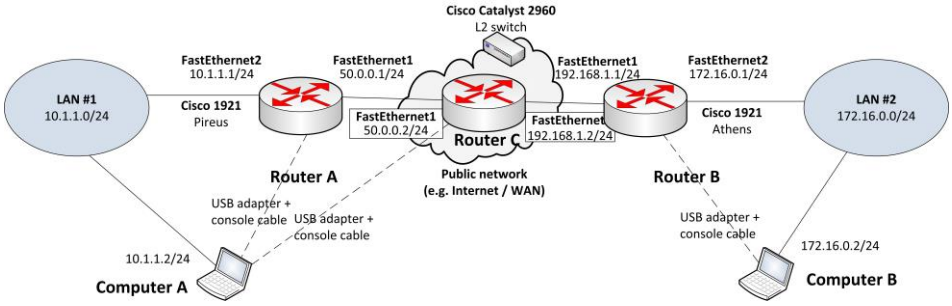

Fig. 7 Laboratory components for VPN lab based on Cisco routers

The second step is configuring simple Site-to-site VPN on two edge routers. The specific scenario used with the Cisco platform is presented at Fig. 7. The differences in IP addressing are presented at the figure as well.

5. The lab exercises

This section is divided in three subsections. In the first subsection, the flow of a lab exercise in non-encrypted network is described. In the second part, a flow of the lab exercise in the encrypted network with established VPN tunnel is described. The benefits of the tunneling the traffic over the public networks are presented with the usage of Wireshark tool for network traffic analysis. The presented steps are similar for both scenarios.

5.1. Using the non-encrypted network scenario

After finishing the first phase of configuration, with IP addressing and static routing, the simple access to the Computer B FTP server is made from Computer A using any FTP client. The network traffic between the computers A and B is monitored by the Wireshark installed on computer A.

By analyzing the network traffic, captured packets, and using option Follow TCP Stream in Wireshark the students are able to see that the username and password are visible to the user of the Wireshark program or to the potential intruder.

5.2. Using the encrypted network scenario

The same set of steps is repeated again with the encrypted network scenario. In this case, network traffic was visible, but the packet content is not visible, which is presented at Fig. 8.

5.3. The experiment and the experience

The experiment with analysis of presented lab exercises usability is made with four students working as a two groups of two. The main reason for including only four students in the exercise is limited equipment, because in this phase only one set of the presented lab equipment is available. All students successfully finished both lectures and lab exercises. These lab exercises are made during the course of Data and Networks Security at Master Degree curricula for Information Technology students. The course is elective.

After the completed exercises, the interviews with students were conducted. The detailed description of a qualitative empirical study with the students is given in the following section.

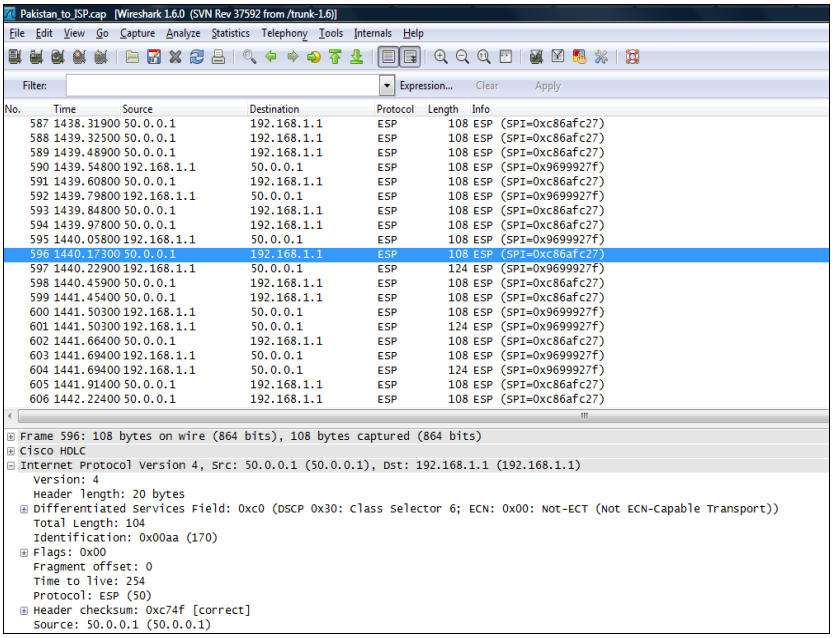

Fig. 8 The Wireshark listing the captured encrypted packets without its content

6. Small scale qualitative study

A qualitative empirical study was conducted in order to enable exploration of students' experiences in using VPN systems in an engineering educational environment. Due to the small number of potential participants that used the educational environment, the only possible option was to use qualitative methods. However, this small number of participants put obvious constraints in designing a study. These constraints were considered through careful selection of research methods and multi-staged qualitative data analysis conducted by three researchers: a leading researcher of the whole research project (the lecturer at the course), an experienced qualitative researcher, and a novice qualitative researcher.

Due to the obvious constraint with the number of participants, the sampling was based on asking potential students to participate in the research. The total number of potential participants (suitable population) was 4, and all of them accepted to participate in the study. The students reported some theoretical and practical previous experiences with computer networks and wireless networks, while nobody reported any experience with VPN systems. The participants only heard about them, but without understanding concepts. Having that in mind, the authors did not expect to achieve saturation of data and developed categories as it is suggested for qualitative studies [13]. This can be considered as a serious threat to the trustworthiness of the findings.

Semi-structured in-depth interviews were selected as the most appropriate method for collecting participants' experiences [12]. Since the number of participants was small, the aim of in-depth interviews was to capture as much details about their experience as it was possible. By thinking in this line, selection of a simple and straightforward data analysis approach was the next important decision, which led to the selection of a general inductive approach proposed by Thomas [11].

6.1. Research Process

Research process was specified in a detailed study design. The main phases in the empirical study are: preparation of the study, conducting the study - collecting and analyzing data, developing the findings, and reporting.

The preparation phase resulted with the detailed design containing: justification for sampling approach and selected research methods, preparation of Informed consent document for ensuring respect of ethical issues [7], and rough draft of data collecting and analysis activities. The phase of data analysis was implemented as a set of iterative activities with highly flexible ordering, as it is usual in qualitative studies [8]. Data analysis included individual work of researchers, as well as joint discussion of all emergent issues in data analysis. The data analysis was implemented by two qualitative researchers, while the leading researcher assisted in refining final category names.

6.2. Empirical Findings

Empirical findings emerged through qualitative data analysis resulted with a framework with categories related to participants' experiences with VPN systems in a wireless network laboratory. Categories are organized within a theoretical descriptive framework.

The main categories relate to direct students' experiences within the laboratory. The following fine categories were developed:

- *Experience in using learning material* - different sources and types of learning materials were identified, requiring students to search for the most appropriate solutions in the laboratory exercises.
- *Experience in solving problems* - different types of problems were identified, leading to different effects for students.
- *Experience in using scenarios for learning* - scenarios of different complexities were used in the laboratory for presenting different technologies to the students.
- *Experience in using Lab sets* - laboratory sets contain active and passive equipment, as well as variety of software tools, enabling implementation of networking scenarios.
- *Experience in implementing VPN* - two platforms were used for presenting the importance of VPN for secure communication in a way that is easy for understanding.

The last segment of the empirical research includes lessons learned during the course, which is important for future professional engagements of the students. Students

reported that laboratory scenarios with implemented VPN helped them to understand concepts that were completely new for them. Based on that understanding they are able to perceive the benefits of implementing VPN in different organizations and business context.

6.3. Trustworthiness

Trustworthiness relates to confidence towards a study findings, and can be judged in terms of credibility and transferability [9]. The main threat to the trustworthiness in this study is small number of participants, causing problems with the saturation of the data.

The first concern is credibility, which should ensure deriving plausible information from the raw empirical data obtained from the participants. Credibility was increased by using the following techniques: writing reflective notes about the all aspects of the research by two researcher engaged in qualitative data analysis, joint work of two researcher with mutual checks of each other findings in all stages of data analysis, refinement of developed categories with the leading researcher in this research project, and through member check with two participants [14]. At the other hand, transferability was not considered in study design, since the objective of the study is experience in the given context (laboratory). However, the design of the study may be replicated in similar educational settings, which will confirm or deny its usability.

7. Conclusion

In this paper, a model of building a laboratory environment for VPN topics and networks security courses is presented. This research is motivated with the importance of network communication security and secure data transfer for all sorts of networks, especially in industrial and business environments.

The laboratory equipment is based on Allen-Bradley® Stratix 5900 service router and its implementation of VPN tunneling, and Cisco platform. The laboratory sets and associated exercises were tested with four students. All students successfully completed the exercises, justifying that the sets are functional and efficient to be used in laboratory courses. All students stated that this environment provided them deep insight into VPN principles and its benefits. The environment enables students to acquire several engineering skills and deep technical knowledge.

Empirical evidence on students' experience with VPN systems in laboratory exercises is presented as a framework with the categories identified through qualitative data analysis. The findings revealed that students found gained skills and experience useful for their future professional career. However, the authors are aware that long term use, improvements and evaluations of the laboratory are necessary for gaining the more reliable view of the laboratory usefulness. This view should be based on few-years longitudinal study that takes into account snapshots for few generations of students [10].

The possible extension of these lab exercises can be made towards the inclusion of exercises with different lab scenarios based on industrial equipment, such as education

PLC controller kits or similar features in order to make stronger connection of the lab exercises and lessons learned to the industrial environments.

Acknowledgment

This research is made possible with the courtesy of Tehna d.o.o., Ljubljana, Slovenia, which provided Allen-Bradley® equipment for laboratory exercises.

This research is supported by Ministry of Education and Science of the Republic of Serbia under the project number TR32044 “The development of software tools for business process analysis and improvement”, 2011-2016.

8. References

1. Allen-Bradley® Stratix 5900™ Services Router, Rockwell Automation, Inc., 2013.
2. Stratix 5900 Services Router User Manual, Rockwell Automation, Inc., USA, 2013.
3. Catalyst 2950 Switch Hardware Installation Guide, Cisco Systems, Inc., USA, 2004.
4. Sanders, C., Practical Packet Analysis: Using Wireshark to Solve Real-World Network Problems 2ed, No Starch Press Inc., USA. (2007)
5. Bullock, J., Kadijk, J.: Wireshark for Security Professionals: Using Wireshark and the Metasploit Framework 1ed, John Wiley & Sons, Inc. (2015)
6. Hooper, H., Matei, C.: CCNP Security VPN 642-648 Official Cert Guide 2ed & Quik Reference, Cisco Press, USA. (2012)
7. Guillemin, M., Gillam, L.: Ethics, Reflexivity, and "Ethically Important Moments" in Research. Qualitative Inquiry, Vol. 10, No. 2, 261-280. (2004)
8. Marshall, C., Rossman, G. B.: Designing Qualitative Research, Fifth Edition. SAGE Publications, Thousand Oaks, CA, USA. (2011)
9. Anney, V. N.: Ensuring the Quality of the Findings of Qualitative Research: Looking at Trustworthiness Criteria. Journal of Emerging Trends in Educational Research and Policy Studies, Vol. 5, No. 2, 272-281. (2014)
10. Bauer, K. W.: Conducting longitudinal studies. New Directions for Institutional Research, Vol. 2004, Issue 121, 75–90. (2004)
11. Thomas, D. R.: A General Inductive Approach for Analyzing Qualitative Evaluation Data. American Journal of Evaluation, Vol. 27, No. 2, 237-246. (2006)
12. Rabionet, S. E.: How I Learned to Design and Conduct Semi-structured Interviews: An Ongoing and Continuous Journey. The Qualitative Report, Vol. 16, No. 2, 563-566. (2011)
13. Guest, G., Bunce, A., Johnson, L.: How Many Interviews Are Enough?: An Experiment with Data Saturation and Variability. Field Methods, Vol. 18, No. 1, 59-82. (2006)
14. Buchbinder, E.: Beyond Checking: Experiences of the Validation Interview. Qualitative Social Work, Vol. 10, No. 1, 106–122. (2011)
15. Petrič, Ž., Dobrilović, D., Žurma, D., Stojanov, Z., Odadžić, B.: Creation of VPN laboratory exercises for industrial Ethernet communication, Proceedings of International conference on applied internet and information technologies, pp. 152-155, October 23, (2015)