Emulating Network Infrastructure

Degree Thesis
submitted to the Faculty of the
Escola Tècnica d'Enginyeria de Telecomunicació de Barcelona
Universitat Politècnica de Catalunya
by

Gerard Peris Olasz

In partial fulfillment
of the requirements for the degree in
Telecommunications Technologies and Services **ENGINEERING**

Tutor : Burcik Jaroslav
Supervisor : Juan Luis Gorricho Moreno
Prague, January 2023

Contents

List of Figures 4

List of Tables 4

1 Introduction 8
1.1 Statement of purpose . . . 8
1.2 Requirements and specifications . . . 8
1.3 Methods and procedures . . . 9
1.4 Work plan and Gantt Diagram . . . 10
1.5 Deviations . . . 10

2 State of the art of the technology used or applied in this thesis: 11
2.1 OpenVPN . . . 11
2.2 EVE-NG . . . 11

3 Practical part 12
3.1 Introduction . . . 12
3.2 Computer configuration . . . 12
3.3 Platform investigation . . . 13
3.4 Creation of labs . . . 15
3.4.1 Procedure . . . 17
3.5 Configuration of labs . . . 21

4 Theoretical research. EVE-NG. 23
4.1 Introduction . . . 23
4.1.1 Emulator vs Simulator . . . 23
4.1.2 EVE-NG . . . 24
4.2 Best Network Emulator / Simulator Tools . . . 24
4.3 Meeting with Uldis Dzerkals, EVE-NG CEO. Questions and Answers. . . . 25
4.4 SMEs . . . 26
4.4.1 What are SMEs? . . . 26
4.4.2 SMEs and EVE-NG . . . 26
4.5 Conclusions . . . 26

5 Theoretical research. Physical vs Virtual switch. 28
5.1 Introduction . . . 28
5.1.1 What is a switch? . . . 28
5.1.2 Types of switches . . . 28
5.1.3 Features . . . 29
5.2 Physical switch . . . 30
5.3 Virtual switch . . . 31
5.3.1 Types of virtual switches . . . 31
5.4 Differences between physical, virtual and virtualized switch . . . 33
5.5 Conclusions . . . 34

6 Network virtualization 35
6.1 Introduction . . . 35
6.2 Benefits and advantages . . . 35
6.2.1 Virtual servers . . . 36
6.2.2 Virtual switches . . . 37
6.3 Conclusions . . . 37

7 Experiments and results 38
7.1 Initial configuration . . . 39
7.2 Tasks . . . 40
7.3 Task 1 - Step 1 . . . 40
7.3.1 Task 1 - Step 2 . . . 41
7.3.2 Task 2 - Step 1 . . . 41
7.4 Task 2 - Step 2 . . . 42

8 Budget 43

9 Conclusions 44

10 Future Work 44

References 45

List of Figures

1 Gantt Diagram . . . 10
2 Schema of how the connection to the EVE-NG console was established. . . 12
3 Three different scenarios. . . . 15
4 Challenge Lab . . . 16
5 Option list . . . 17
6 Different vendor templates for a new node . . . 17
7 Node properties . . . 18
8 Network Infrastructure scenario . . . 21
9 First MAC Bridge introduced by Mark Kempf in 1983. [1] . . . 30
10 Brief scheme of how a physical switch looks and works in today's world. [2] 30
11 Scheme image about how virtual switches work. . . . 31
12 Lab 3.5.1: Basic VLAN Configuration . . . 38
13 Information about the predefined configuration of the scenario. . . . 39
14 Three different scenarios. . . . 40

List of Tables

1 This table shows the main differences between emulation and simulation platforms. [3] . . . 23
2 The table is a comparison among the best network emulator and network simulator tools. [4] . . . 24
3 Difference between managed and unmanaged switches. [5] [6] . . . 28
4 Different types of virtual switches. [7] . . . 31
5 This table shows the main differences physical and virtual switches.[8] . . . 33
6 Table showing the budget considered during the development of the Thesis. 43
7 Total amortization related to materials. . . . 43

Abbreviations

2FA Two-Factor Authentication

AD Active Directory

CEO Chief Executive Officer

CTU Czech Techinical University

DB DataBase

ESXi Elastic Sky X integrated

EVE-NG Emulating Virtual Environment - Next Generation

GNS3 Graphical Network Simulator - 3

IP Internet Protocol

L2 Layer 2

L3 Layer 3

LAN Local Access Network

NET Network Emulator Tool

NIC Network Interface Card

NST Network Simulator Tool

NVRAM Non-Volatile Random Access Memory

OpenVPN Open Virtual Private Network

OSI Open System Interconnection

pdf Portable Document Format

RADIUS Remote Authentication Dial-In User Service

RAM Random Access Memory

RDP Remote Desktop Protocol

SMEs Small and Mid-size Enterprises

SSL Secure Sockets Layer

TCP Transmission Control Protocol

TLS Transport Layer Security

VPN Virtual Private Network

Abstract

In today's world, every existing enterprise must have a network infrastructure in order to be able to communicate between their private network and the public network. Network emulation / simulation is one way to design the private network infrastructure with all the detail needed for this kind of job, as you can design it in advanced reducing almost to zero the probability of committing an error during the process as well as test the configuration before implementing it.

In this written work, you will find information about these kind of platforms, specifically about EVE-NG, as well as my own experience using it. Moreover, you will also find information about the main differences between physical and virtual switches, as well as an explanation of network virtualization, its benefits and the most relevant aspects that make this networking concept a huge deal for today's IT world requirements.

Revision history and approval record

Revision	Date	Purpose
0	24/10/2022	Document creation
1	16/01/2023	Document revision

DOCUMENT DISTRIBUTION LIST

Name	e-mail
Gerard Peris Olasz	gerard.peris@estudiantat.upc.edu
Juan Luis Gorricho Moreno	juan.luis.gorricho@upc.edu
Burcik Jaroslav	burcik@itu.fel.cvut.cz

Written by: Gerard Peris Olasz		Reviewed and approved by: Juan Luis Gorricho Moreno	
Date	24/10/2022	Date	16/01/2023
Name	Gerard Peris Olasz	Name	Juan Luis Gorricho Moreno
Position	Project Author	Position	Project Supervisor

1 Introduction

The project has been carried out at the Network Security Department of Faculty of Electrical Engineering, Czech Technical University in Prague.

The purpose of this project is to create virtual network infrastructure in order to provide future students some scenarios to practice its configurations.

Moreover, two theoretical researches have been done; the first one about the platform that will be used during this project, about its strengths and weaknesses compared to its competitors. The second one, about the differences between physical and virtual switches.

1.1 Statement of purpose

The project main objectives are:

1. To learn about the pros and cons of a network infrastructure emulator for the creation of different kinds of scenarios. This will not only provide an opportunity for new students to practice their network configuration skills but also for cybersecurity purposes, such as vulnerability management.
2. To understand the different layers that form a network infrastructure, this is how they interact with each other by the configuration of the different scenarios.
3. To study the differences between a virtual switch and a physical one, its benefits and deficiencies.
4. To analyze the impact that this kind of platforms could have on the business environment, mainly on Small and Mid-size Enterprises (SME), as well as to analyze their competitors.
5. To analyze the current impact that network virtualization is having, its benefits as well as its most relevant aspects.

1.2 Requirements and specifications

Project requirements:

The project will follow the guidelines marked by the agreement achieved between my supervisor and me. There will be some requirements with big weight, so they will be mandatory to fulfill. Some of them are:

- The designed scenarios will be done with the help of EVE-NG, a virtual network infrastructure emulator.
- The designed scenarios will have different levels of difficulty.
- The scenarios have to be designed in order to be solvable by a student, that means that they have to have some basic information in order to be configured.
- To have basic notions about network infrastructure and its devices.

- There must be a good learning curve with the emulator tool in order to be able to create difficult scenarios with the minimum time needed.
- To have a good level of English, in order to be able to properly communicate with my supervisor and its team and to fully understand the emulator tool that will be used during the project.

Project specifications:

After defining the needed requirements, we are going to establish the specifications to accomplish the previous requirements:

- To have internet connection in order to be able to use the network infrastructure emulator tool. The connection will be established through a VPN have direct connection to the specified computer via RDP.
- To understand the functionalities of the network infrastructure emulator in order to be agile and precise in the creation of the scenarios.
- Understanding how a network infrastructure works is needed to create scenarios with different levels of difficulty.
- By having a guidebook given from my supervisor, the specifications that each scenario must have will be fully implemented.
- By practicing with simple scenarios, the learning curve will be in accordance with the time period needed to complete the project.
- By having experience speaking and studying English, the communication with the supervisor and its team will be easily carried out. Moreover, this will also help to understand in a better way the emulator tool.

1.3 Methods and procedures

During this thesis, an emulation platform has been used called EVE-NG. This platform was previously developed by Uldis Dzerkals, EVE-NG CEO, and his software engineering team.

It evolved from another project called UNetLab, and the basis of their code came from the open source code emulation platform called GNS3.

1.4 Work plan and Gantt Diagram

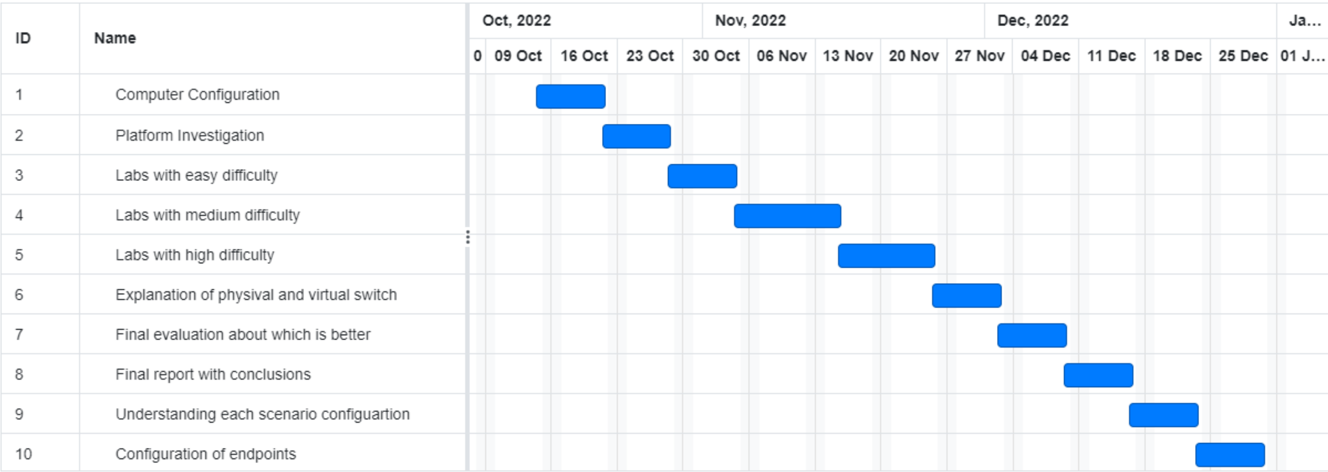


Figure 1: Gantt Diagram

1.5 Deviations

During the development of this project, some deviations have occurred from the initial plan. These deviations appeared due to some specific changes of the project scope and punctual delays when giving new material to work on.

- The first deviation was about WP2. In the initial plan, the number of labs that were supposed to be designed was much less than the real total number of labs that were finally created. This is because the destination university supervisor gave extra labs to design as he saw that the learning curve when creating the different scenarios was good enough to give additional labs to create. As a consequence, the time spent designing those labs was more than expected on this part of the project.

- The second deviation was about WP3. This work package corresponded to the configuration of the different scenarios that have been designed during the Thesis. It was supposed to have them configured before starting the theoretical part of the project, this is the two theoretical researches, but the theoretical part was carried out before the configuration of the scenarios. That means that WP3 comes after WP4 and WP5.

- The last deviation of the initial plan was the extension of the WP5. Initially, this work package was about EVE-NG and the impact that it has on SMEs, but a decision was made in order to extend it to a platform investigation where a description and a comparison between other similar platforms was added. Moreover, a meeting with the EVE-NG CEO took place. As a consequence of this extension, the time spent working on this part was prolonged.

2 State of the art of the technology used or applied in this thesis:

2.1 OpenVPN

During the development of the Thesis, the OpenVPN application has been used in order to establish an open VPN connection to the servers of the CTU.

This application was created by James Yonan and developed by the OpenVPN project / OpenVPN Inc. It is a full-featured SSL VPN which implements OSI layer 2 or 3 secure network extension using the industry standard SSL/TLS protocol, supports flexible client authentication methods based on certificates, smart cards, and/or username/password credentials, and allows user or group-specific access control policies using firewall rules applied to the VPN virtual interface.

The introduction paper [9] had to be read in order to fully understand how these kind of protocols work. The content of this introduction paper is a brief summary of how it works, and it is located in the official web page of the application.

Moreover, the write up guide had to be followed[10] in order to make the real connection. The Thesis supervisor's sent the necessary certificates and keys for the OpenVPN configuration. Then, the web page step-by-step guide was followed and the connection was successfuly established.

2.2 EVE-NG

EVE-NG is a network infrastructure emulation platform that I have been using during the whole development this Thesis. Previous to its usage, the platform's official website contained a *Documentation* tab were you can get a basic idea of how the platform works.

Once the basics of the platform were assimilated, a testing of the different features began. At first, there were some troubles of how to use it, so the platform tutorials were really good aid[11] because watching them would help to understand the topology used in the platform, as well as basic functionalities such as creating labs and connecting different nodes.

Later on, the creation of the first official labs began with the aid of some documents that the Thesis supervisor sent. Some trouble while designing them appeared, as these documents seemed to be lacking a little bit of information for the creation of the labs, so a search for more consistent information of the platform took place. After a while, the EVE-NG Professional Cookbook [12] was found which contained indeed the missing information.

It contained information about their web topology page, the web GUI management, about their consoles or their usage (with some examples included). All the information was really good not only because it helped for carrying out the practical part of the Thesis but the theoretical as well.

3 Practical part

3.1 Introduction

The project that has been done during the Thesis was the creation of different network infrastructure scenarios for incoming students next semester. The design of them had to be done using an emulation platform called EVE-NG, with which you can create this kind of scenarios and configure them to test its functionality.

These scenarios will be used for educational purposes, for students to test and improve their skills when configuring different network devices such as switches, routers, endpoints and so on.

3.2 Computer configuration

The first part of the project consisted on configuring the computer that had to be used for the development of this Thesis in order to get access to the CTU private network, as the servers that manage EVE-NG are located there.

First of all, an OpenVPN connection was mandatory to get access to the CTU servers. After receiving the necessary certificates and keys for the configuration from the supervisor, a search for how the connection had to be established began, as there was no previous knowledge about how to do so. An application called OpenVPN was found and it seemed to fit the requirements, as the application could be downloaded for free and had a step-by-step guide to help with the configuration.

Later on, the supervisor sent a pre-configured VM image in order to be able to connect to the native console of the platform. On the contrary to the OpenVPN application, the previous experience using this kind of VMs made easier the installation of it and gave no problem when using it. VMware was the workstation used to install the image.

Once everything was set up, the supervisor showed how to make a reservation to one of their *pod's*. These *pod's* where the different EVE-NG consoles that they had active in order to use the platform, so a reservation of one of them had to be made in order to be able to use the platform. This reservation had to be done in advanced.

Here you will find a schema of how the CTU network infrastructure is distributed, in order to understand in a proper way how the connection from my personal laptop worked:

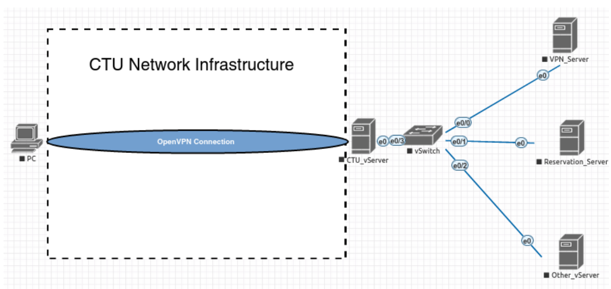


Figure 2: Schema of how the connection to the EVE-NG console was established.

As the schema shows, the OpenVPN connection went directly through the CTU Network Infrastructure to a virtual server. This virtual server had direct connection through a virtual switch to other servers. The image shows servers such as the reservation server, with which you could make the corresponding reservation of the *pod's* consoles of EVE-NG, as well as the OpenVPN server and other servers. The *pod's* are installed into different VM's, and these VM's are all interconnected through a virtual switch.

3.3 Platform investigation

At this point of the project, the design of the labs that the supervisor and his assistant proposed as a task for the project had to began. At first, it was difficult to manage through the platform, as there was a lack of experience when using emulation / simulation platforms.

Because of this, additional useful information had to be found on the Internet in order to help out with the basics steps for creating such scenarios. The home official web page of EVE-NG had a lot of useful tutorials and documents for a beginner to use. These videos and documents can be found in the references of this Thesis, as they have been previously cited in the *State of the art of the technology used* section.

After acknowledging the basics functionalities of the platform, it was time to start "playing" with it in order to gain more experience when using it before starting with the creation of the first official laboratories. As a consequence, some functionalities that didn't appear in the tutorials were difficult to use, so there was a need to understand and manage them. These functionalities were not as relevant as the ones that the tutorials showed you up, but they did make a difference when talking about the configuration of the different network devices.

These functionalities were modifying the devices properties such as the number of on the nodes, the RAM that you want them to have, the number of Ethernet interfaces, the startup configuration that you want them to have or simply the node icon that appears on the Topology. Thanks to the *Professional Cookbook* document of EVE-NG, these functionalities were successfully understood and it was possible to continue with the different demands of the laboratories scenarios.

After that, the features and relevant characteristics of the platform were important to learn about them in order to not only understand even better how the platform is designed and its capabilities but as well for the theoretical research of the platform. Again, in his own website they had a tab for the features divided into key features and objectives, in which they make a difference between community edition and professional edition. The most relevant aspects of both are listed in the EVE-NG theoretical research.

Therefore a question came up: is this the best platform for doing this kind of job? The aim with this question was to evaluate the different competitors that EVE-NG has, because apart from the fact that the platform is pretty much good, as they have a lot of support for inexperienced people, and the learning curve is really soft, there could be the possibility to find other platforms with better features and characteristics. A search for similar platforms that were available in today's IT market sector began, and it ended up showing more or less the same five platforms in every article or website that talked about it. These platforms are listed and compared in the first theoretical part of the project.

Last but not least, some questions about the platform that could not be answered by the Internet arose. Because of this, a decision was made to contact with any worker of the platform, as they had a support tab on it where you could simply send them an email with your doubts. Surprisingly, the person that answered the email was Uldis Dzerkals, the CEO of EVE-NG, and his answer to the meeting proposal was positive. You will also find a summary of the meeting in the theoretical part of EVE-NG.

We have to take into consideration that the purposes for this platform investigation were not only to learn the basic functionalities of the platform but for the future theoretical research about it. That's why it took pretty much long to do it.

3.4 Creation of labs

Once all the basic functionalities were assimilated, it was time to start working on the different network infrastructure scenarios that the Thesis supervisor gave to work on. The decision of dividing them into levels of difficulty was taken, resulting in a total number of three levels: **easy**, **medium** and **high**. This differentiation of difficulty was premeditated, which means that different aspects of the scenarios were considered in order to classify them, such as the number of different devices connected to the network, the approximate necessary time for solving it or the difficulty of its configuration, which is normally based on the complexity of the whole infrastructure itself.

In order to make easier the improvement on the skills on the platform and gain more experience with it, the designing of the scenarios with an **easy difficulty** level was the first commitment. These labs were:

- **Lab 2.6.1**: Basic VLAN Configuration.
- **Lab 3.5.2**: Subnetting Scenario 1.

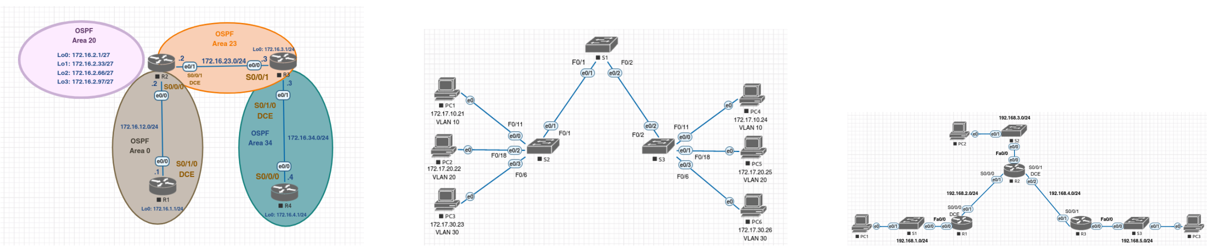
After finishing the first laboratories, the next step was the creation of the **medium difficulty** ones, which were:

- **Lab 5.6.1**: Basic RIP Configuration.
- **Lab 2.8.1**: Basic Static Route Configuration.

Moreover, once medium difficulty scenarios were finished, it was time to began with the **high difficulty** ones. These high difficulty scenarios were really different from the ones that had been done, as the complexity of the network infrastructure was considerably higher. These labs were the following ones:

- **Lab 3-5**: OSPF Challenge Lab.
- **Lab 7.4.1**: Basic DHCP and NAT Configuration.
- **Lab 4-1**: Redistribution Between RIP and OSPF.

The following figures show the difference between each level of scenario difficulty:



(a) **Easy difficulty.** OSPF Challenge Lab

(b) **Medium difficulty.** Basic VLAN Configuration

(c) **High difficulty.** Basic RIP Configuration

Figure 3: Three different scenarios.

After finishing all the labs, there was more time than the expected for this part of the project, as they had all been finished up before time. After talking to the supervisor and showing him up the results, he decided to give extra scenarios to design, all of them of high difficulty or above, as their complexity and detail were equal or higher than the high difficulty that were given at the beginning of the project. He gave a total number of 6 more labs to design. These were the following:

- CCNA Routing and Switching Scaling Networks
- CCNP-sec-Tunels
- Challenge Lab
- Lab 6-3: Securing VLANs with Private VLANs RACLs and VACLs
- MPLS VPN over DMVPN
- OSPF

The difference between the previous designed labs and these new ones is clearly shown on the time spent, as high difficulty laboratories took approximately one hour each, maybe a little bit more, but the last ones it took more than two and a half hours for each one of them. You will now see a picture of one of the laboratories.

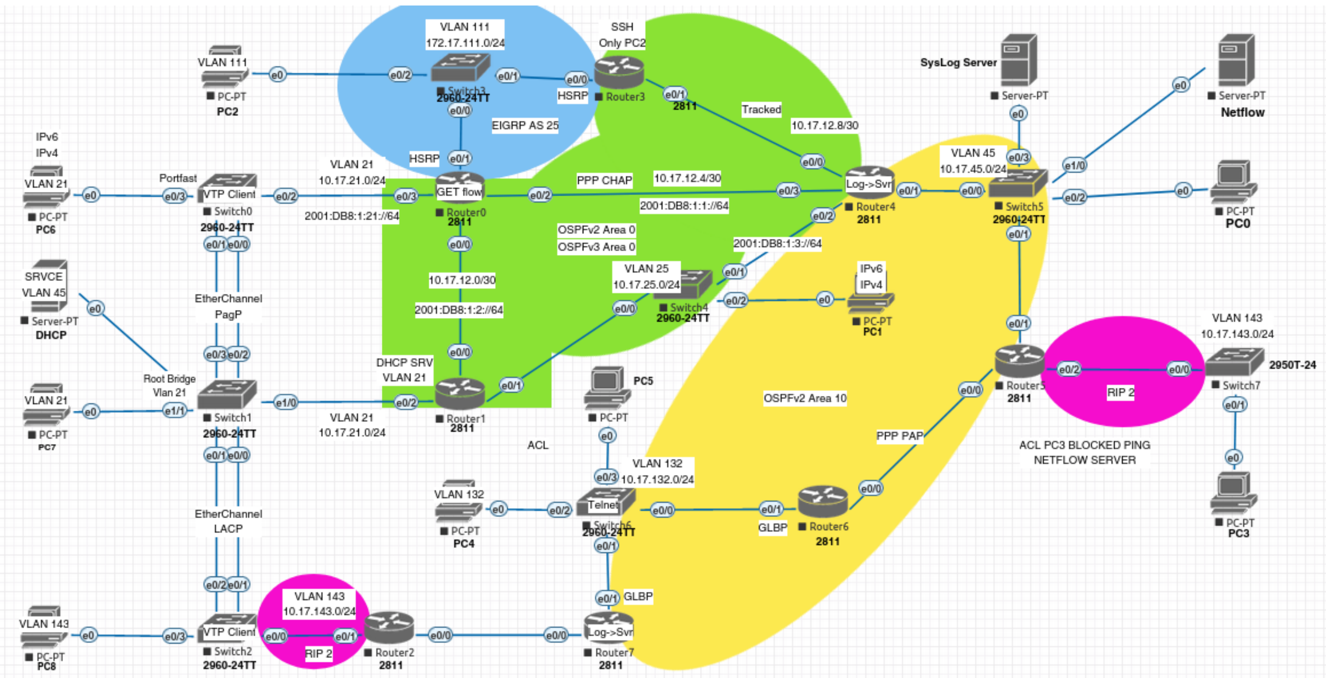


Figure 4: Challenge Lab

3.4.1 Procedure

In this subsection, an explanation of the procedure followed during the development of the different laboratories will take palce. It has to be considered that more or less, independently of the difficulty of the lab, the process has been the same.

First of all, a reservation of one of the *pod's* had to be made in order to gain access to the virtual emulator. This reservation was made from one of their servers, so the OpenVPN connection had to be running in order to do so. There was the need to specify some aspects of the reservation, such as the title of it and the period of time that the *pod* was going to be used, and the reservation had to be done in advanced. For example, if you wanted to use it from 11:00 to 14:00 but it was already 11:05, you had to make the reservation from 11:30 to 14:00.

Once the reservation time began, it was able to access through a private IP to the specified *pod* and enter, with the given credentials by the supervisor, to the emulation platform. When right clicking in the platform, the following option list popped up:

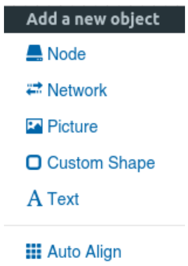


Figure 5: Option list

This list was everything needed to design the labs. To begin with, you had to start by selecting the *Node* option, with which you could select the different devices to add, as well as the template that they would be using. For example, in Figure 2 - (b), we can see three different switches and six endpoints. These devices could have the following templates from different vendors:

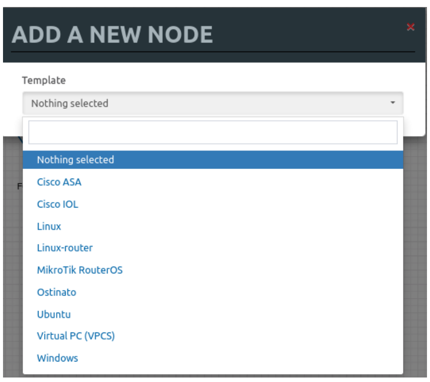


Figure 6: Different vendor templates for a new node

In this case, the Cisco IOL template was used for switches and routers while the Linux one was used on endpoints and Windows for servers. The decision of using one or other was purely a decision of one's own, as the supervisor stated it didn't matter what templates to use as long as switches and routers used the Cisco IOL one.

Once you had the template for your new node, the platform redirected you to a new window. This window looked like this:

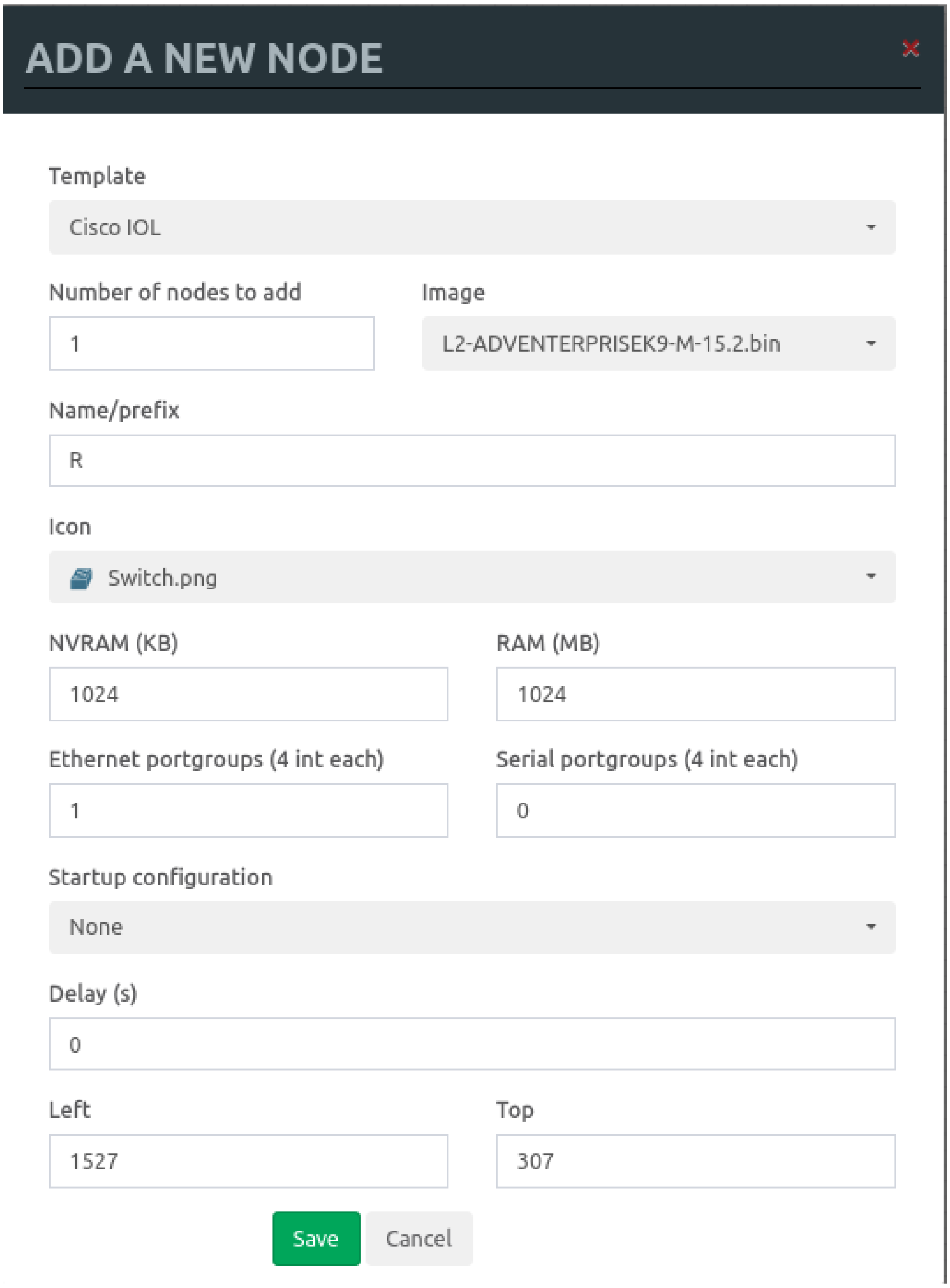


Figure 7: Node properties

As it can be seen in the above figure, each node has some properties that can be modified. Some of this properties had already been mentioned during the previous section, about platform investigation, but let's take a deep look at each one of them:

- **Template:** This one was just mentioned before, it is used for changing the template used on that particular node.
- **Number of nodes to add:** As the own property says, you can add multiple nodes with the same properties at once, saving a lot of time if this is the case.
- **Image:** This option permitted choosing between the different vendor template images. In the case of Cisco IOL template, two options were available; the first one was the one that can be seen on the figure, used for acting as a switch, as it is a L2 device. The second option was a L3 image, meant to act as a router device instead.
- **Name/prefix:** It was used for recognizing the different devices. It could be modified for any name and if multiple nodes were added they would have the same name followed by a number in order to make a differentiation between them.
- **Icon:** Purely visual, this function only modifies the icon that can be seen on the platform, but obviously there are as icons as devices you may use in the designed scenario.
- **NVRAM:** The NVRAM value could be changed depending on your own needs. NVRAM is used as writable permanent storage for the startup configuration. During the boot process, the node will always check NVRAM for a saved configuration.
- **RAM:** Each node template has a pre-set RAM value that aligns with vendor requirements. This value is displayed in MB and may be changed per your needs.
- **Ethernet portgroups:** Each node had, by default, 1 Ethernet portgroups, which meant that only 4 interfaces were available on that particular device, going from e0/0 to e0/3. However, more interfaces could be added by increasing the number of Ethernet portgroups. For example, if that was a 2 we would have 8 interfaces. If it was a 3 then 12. The increase was 4 by 4.
- **Serial portgroups:** The serial interface option is available for IOL nodes only and follows the same grouping structure as Ethernet interfaces. A value of 1 for Serial means your node will have 4 serial interfaces.
- **Startup configuration:** If needed, a startup configuration could be directly exported to the node.
- **Delay (s):** The Delay value is set in seconds and can be used to delay a node from booting after it is started. Example: if the value is set to 30, the node will wait 30 seconds before processing its boot sequence.
- **Left and Top:** These two options function is to indicate their position in the scenario.

Having said all that, the modification of these properties was not necessary at all, except the basic ones, as the supervisor clearly indicated that the default configuration was good enough for the students that will be configuring these network infrastructure scenarios.

After adding the different nodes, it followed making the different connections between the different devices. By left clicking on the devices and dragging the cursor to the other device that you wanted to make the connection, a new window appeared where you had to select the different interface that the devices were going to use for the exchange of data frames when running the emulation.

Therefore, it was mandatory to modify the different default names of the devices for the ones that appeared in the given pdf. This was accomplished by clicking on the *Text* option of the option list and dragging the respective text to wherever it had to be placed.

Last but not least, the addition of any instructions about the network infrastructures had to be done, such as the different IPs of the devices, the VLANs that were using, the protocol that they followed or make a graphical identification of the different subnets, as it can be seen in Figure 3, they were divided by colors, in order to make it easier for the students to complete the laboratories. The division of the subnets were made with the *Custom Shape* option of the option list, where you could select if you wanted a circle or a square as well as the color that they had to have, its shape and outline.

3.5 Configuration of labs

In this subsection we will be dealing with the configuration of a network infrastructure scenario personally designed in order to show some of the basic commands to properly configure a network infrastructure. Some functionalities will be shown, such as the creation of VLANs and interfaces, enabling and disabling the ports, showing up the present configuration or simply assigning IP addresses.

The following image shows the case scenario that is going to be configured.

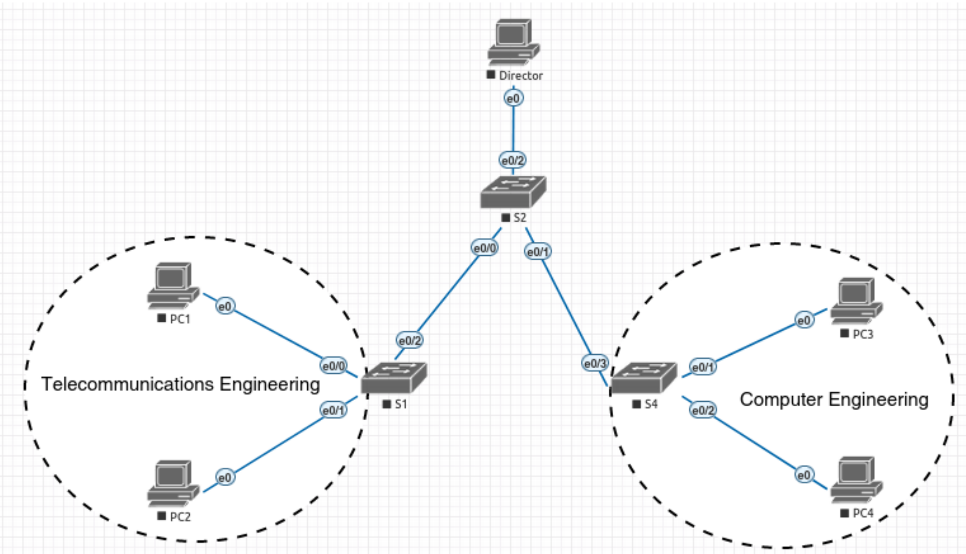


Figure 8: Network Infrastructure scenario

The aim of this configuration will be to show some of the most basic switch configurations, which will be:

- Create two different VLANs on S2 in order to correctly distribute the data frames, as well as assign them a name.
  - **Procedure:** First of all, enter on *EXEC mode* by typing ***enable***. Then, type ***config terminal*** to enter into the configuration of the terminal. Afterwards, by typing ***vlan 10***, then ***name Telecos***, the VLAN Telecos will be automatically created.
- Assign each one of the VLANs interfaces an IP address.
  - **Procedure:** On *EXEC mode*, and into the configuration of the terminal, we have to type ***interface vlan 10***, ***ip address 10.10.10.10 255.255.255.0***. For the Info VLAN, we just have to do the same but giving it another IP address.
- On S1 and S3, create one VLAN for each of the PCs that are connected to them.

- **Procedure:** As we have seen previously on S2, we have to enter on *EXEC mode* by typing ***enable***. Then, type ***config terminal*** to enter into the configuration of the terminal. Afterwards, by typing ***vlan 40***, then ***name upper***, the VLAN *upper* will be automatically created. We just repeat the same procedure and create a VLAN for the other PC.

- Shutdown the interfaces that are not being used on each of the switches.
  - **Procedure:** On s!, there is only one interface that is not being used, which is **e0/3**, so in order to shut it down, we have to go on *EXEC mode*, type ***config term***, then type ***interface e0/3*** and finally introduce the following command ***shutdown***. This way the interface will no longer be opened.

- Configure a password for EXEC mode and for vty connections.
  - **Procedure:** For EXEC mode password, we have to enter into the config term and then type ***enable password pass***, and the password *pass* will be requested when entering into EXEC mode. For vty connections, we have to enter into the config term, then type ***line vty ?*** in order to know the number of vty lines that we are dealing with. In this case is 0 4, so we type again ***line vty 0 4*** and last we type **password pass** and this password will be settled up for vty connections.

- To save the configuration.
  - **Procedure:** On *EXEC mode*, we just have to type ***copy running-config startup-config*** and the running configuration will be saved in case we reboot the switch.

Some other configuration will be shown in the *Experiments and Results* section.

4 Theoretical research. EVE-NG.

4.1 Introduction

In this first theoretical part of the Thesis, a deep research about an emulator platform called EVE-NG will take place. This platform has been used during the whole development of the final Thesis. First of all, the differences between emulator and simulator tools will be explained.

Afterwards, it will follow an introduction to EVE-NG with a brief description of the platform and its most important features. A comparison between EVE-NG and their competitors will follow the introduction, which are different emulation and simulation platforms that compete with them in this technology field.

After it, a summary of the meeting with EVE-NG CEO where he officially presents the platform and also answers some questions that had been prepared for the occasion. Next there is a review of what SMEs are and the impact that they have had on EVE-NG, the relation that this platform keeps with this type of enterprises.

Last but not least, the conclusion of the written work with a personal point of view of all the information gathered during this investigation.

4.1.1 Emulator vs Simulator

An emulator enables a computer system to mimic the software and hardware, while a simulator models an environment that mimics the behavior and configuration of another target device.

Let's now take a look at the following table in order to spot the difference between these two software devices in an easier way.

Criteria	Emulator	Simulator
Target Area	Emulators target the whole device, that is its hardware, software and Operating System.	Simulators target the mobile device behavior.
Provider	Device manufacturers.	Device manufacturers and other companies.
Internal Structure	Programmed as a real-life device, that is Machine-level (a.k.a Low-level language) assembly language.	Programmed in High-level language.
Usage	Emulators are used to emulate the software and hardware features of a real device; suitable for debugging.	Simulators are used to simulate the behavior and configuration of a real-device; less reliable for debugging.
Performance	Slower perform due to latency as they have binary translation.	Faster perform as it does not has binary translation.

Table 1: This table shows the main differences between emulation and simulation platforms. [3]

4.1.2 EVE-NG

[13] Some years ago, a project called UNetLab was created and few time after it the project was renamed to EVE-NG. EVE-NG is nowadays one of the best emulator platforms for today's IT-world requirements, as with this platform you have the possibility to design different virtual environments for different purposes, such as:

- **Proof of concepts**, as you can design any imaginable scenario in order to prove its value before making a real implementation of it in your enterprise, center, etc.
- **Virtual solutions**, once a design is approved by a customer you start working on EVE-NG to do the virtual solution that will be the final product you present to the customer.
- **Training environments**, for learning purposes or even for testing purposes, as you could emulate your own network infrastructure in order to test it against different cyber security attacks or for practicing network configuration.

The platform provides an unique experience to the client, as it has different features that makes this emulation tool be easy to use. The most relevant features are mentioned in the official written work, annexed to this thesis.

4.2 Best Network Emulator / Simulator Tools

In order to have an accurate view of the potential that EVE-NG has, a comparison between the five best NST and NET will be made. The following table shows the most important characteristics for a network simulator / emulator tool to have:

	Features					
NET and NST Tools	Network virtualization	*Click and Play* Topology	Packet Capture	Real Network Transposing	Clientless	Price
GNS3(E) [14]	✓	✓	✓	✓	×	Free
Cisco Packet Tracer (S) [15]	✓	✓	✓	×	×	Free
EVE-NG (E)	✓	✓	✓	✓	✓	Free
Network Simulator 3 (S) [16]	✓	×	×	×	×	?
Cisco Virtual Internet Routing Lab (S) [17]	✓	✓	×	×	×	200 € / year

Table 2: The table is a comparison among the best network emulator and network simulator tools. [4]

The table clearly shows that EVE-NG is one of the pioneers of this kind of platforms. However, platforms such as GNS3 or Cisco Packet Tracer are really good options as well.

4.3 Meeting with Uldis Dzerkals, EVE-NG CEO. Questions and Answers.

There was the possibility to contact with Uldis Dzerkals, founder and CEO of EVE-NG ltd, in order to ask him some questions about his platform and to complement the most relevant aspects offered on it.

The meeting began with an official presentation of EVE-NG, where he talked about different aspects of the platform such as licensing, the different images used in the platform, their most relevant competitors, the simultaneous usage of it or the advantages of having a cluster system (which means that the platform is built with a multi server environment but the system works as if it was only one server).

Once he finished his presentation, it followed some prepared questions for him. The first question was about the kind of clients they were looking for at the very beginning; Uldis said that at the very beginning of this project, the platform was planned to be used for educational purposes such as professional trainers or university students but they ended dividing it into two directions, but it ended up accomplishing other purposes such as security testing or for corporate usage, the most relevant one, as this platform can be used for testing environments, for creating project prototypes before implementing them.

Afterwards, the next question was about the differences between an emulator and a simulator considering that simulators are generally cheaper than emulators, in order to see if simulators could be used for the same purpose as emulators. He simply said that it was a costumer decision. However, he added that if you want to prepare a real-life situation, an emulator would suit much better, as they use real images which will give you a real experience of how the network would work if it was implemented in real-life.

After this brief introduction, there was the need to know more about the platform features. First of all, the differences between a virtual PoC and a virtual solution were commented, as the platform offers both. Once a design is approved by a customer, you start working on EVE-NG to do the virtual solutions that will be the final product to present to your customer.

The next question prepared to him was about the main features/characteristics of the platform that make it differ from other competitors, and he really liked that question. He made four points:

1. **Scalability,** as the platform has a cluster system which is directly related to the professional edition, you cannot build it without this cluster system.
2. **Full integration with costumer** DB environment, RADIUS, AD, 2FA and more.
3. **Live customer support,** EVE-NG offers customer support for solving doubts and answering any questions related to the platform usage.
4. **Clientless,** which makes this platform unique as other competitors are still trying to achieve the same.

The last question was about his opinion about SMEs as potential clients to the platform. The most relevant aspects are commented in the next section, but to sum up Uldis said that EVE-NG and SMEs have a very good relation, as his company has a lot of business relations with this kind of enterprises.

4.4 SMEs

4.4.1 What are SMEs?

Small and mid-size enterprises (SMEs) are businesses that match a threshold defined by its country. This threshold takes into account some factors such as the maintained revenues, assets or number of employees. [18]

The criteria met for this kind of enterprise can occasionally vary depending on the industry sector. Despite that, we will take into consideration companies with assets below 3 million euros.

4.4.2 SMEs and EVE-NG

After interviewing Uldis Dzerkals, founder and CEO of EVE-NG, it is clear that this platform has a lot of potential for SMEs, not only because of their fair prices and flexibility to their customer demands but because the learning curve is very suitable for the employees that would use the platform.

It would only take between 3 and 6 months for an experienced employee to fully manage himself through the platform. Moreover, the lack of experience should not be a problem because the platform contains a lot of tutorials and support for inexperienced employees.

The industry sector that would take more profit from this platform would be the network security companies, as the platform runs the newest security devices and with most popular vendors. You can create PoC and test different environments with the newest protocols, including newest encryption methods.

Furthermore, network infrastructure companies would also benefit from the usage of this platform, as having the possibility to emulate real-life infrastructures makes this job not only easier and more precise but also risk less.

4.5 Conclusions

To conclude this theoretical investigation of the EVE-NG platform, it is clear that emulation tools are different from simulation tools; it is not about which is better but the reason for using it, as emulators would suit better for more advanced projects and more experienced people, whereas simulators could work for the initial part of a network infrastructure project but it would not be enough for today's IT-world requirements.

Emulators give a real-life user experience. You can design virtual environments that will work as if they were implemented in real life, which means that they are more reliable for debugging. In other words, emulators can guarantee an error free network infrastructure while simulators not that much.

Although EVE-NG has different competitors with pretty good platforms, EVE-NG is one of the best available platforms in the market. It is very complete with some incredibly modern features that allows the user to have a real experience, as having the possibility to replicate a real environment with official vendor images helps the user to commit less errors and, as a consequence, reduce costs.

5 Theoretical research. Physical vs Virtual switch.

5.1 Introduction

The second theoretical part of the Thesis will be about making a difference between physical and virtual switches, which are similar network devices but they have relevant differences.

5.1.1 What is a switch?

A switch is a high-speed device that receives incoming data frames and redirects them to their destination on a LAN. These devices operate at the data link layer (Layer 2).

They read the MAC Addresses from incoming TCP/IP data frames containing port information as they pass into one or more input ports. Moreover, the destination information contained in those frames is used to determine which output port will be used to send the data to its correct destination. [19]

5.1.2 Types of switches

There are two different main types of switches, which are defined in the following table taking into account different components that are relevant when talking about network devices.

Component	Managed switch	Unmanaged switch
Configuration	Open to configuration.	No configuration needed.
Technical skills.	Requires prepared personal for setting it up and for proper maintenance.	Plug and play, no previous knowledge required.
Security	Ability to monitor and control the network to shut down active threats.	They are secured by ensuring you have no vulnerabilities from system to system.
Application	They suit better for enterprises-sized businesses with much larger network scope.	Small networks such as small-sized businesses, your own home, a single office or so on are good scenarios for this kind of switches.
Capabilities	Spanning Tree Protocol support, Quality of Service, bandwidth rate limiting and port mirroring.	Maintains MAC address tables.
Pricing	More expensive.	Less expensive.

Table 3: Difference between managed and unmanaged switches. [5] [6]

5.1.3 Features

Let's now to take a look at the most relevant features that all switches have.[20] These features are:

1. A switch operates in the layer 2, i.e. data link layer of the OSI model.
2. It is a network device that can be conceived as a multiport network bridge.
3. It uses MAC addresses (addresses of medium access control sublayer) to send data frames to the selected destination ports.
4. It uses packet switching technique to receive and forward data frames from the source to the destination device.
5. It supports unicast (one-to-one), multicast (one-to-many) and broadcast (one-to-all) communications.
6. Transmission mode is full duplex, i.e. communication in the channel occurs in both the directions at the same time, or half duplex, depending on the network characteristics.
7. Switches are active devices, equipped with network software and network management capabilities.
8. Switches can perform some error checking before forwarding data to the destined port.
9. In general, the number of ports is higher – 24/48.

5.2 Physical switch

The first MAC Bridge was introduced in 1983 by Mark Kempf. Shortly after it, 2 port MAC Bridge was invented and later multi port MAC Bridge came in. The following schema shows how it worked the first MAC Bridge created by Mark Kempf:

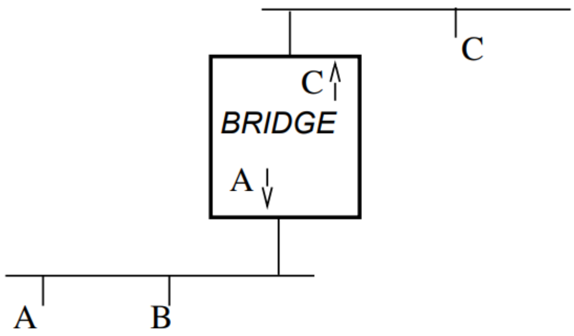


Figure 9: First MAC Bridge introduced by Mark Kempf in 1983. [1]

The bridge should make the two Ethernet look like one big Ethernet, so that when A sends an Ethernet a data frame to C it magically gets to C without A having to even know there is a bridge in the middle.

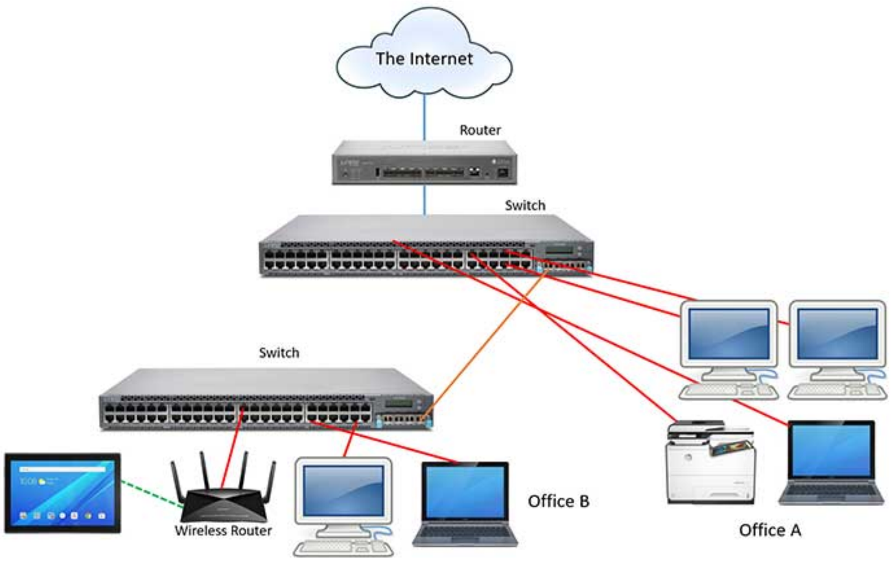


Figure 10: Brief scheme of how a physical switch looks and works in today's world. [2]

At the very beginning, different devices are connected to the first switch. Then, this switch is directly connected through an Ethernet cable to another switch. This second switch can also have devices connected to it, forming another network segment.

5.3 Virtual switch

Virtual switches like physical switches enable network components, like virtual machines, to communicate between them. In this case, virtual machines act as operating systems that imitate hardware devices. Moreover, a virtual switch and its virtualized network adapter are connected to a switch. As a consequence, a hypervisor is needed in order to host multiple virtual machines in a single computer hardware.

The next image shows how a virtual switch works:

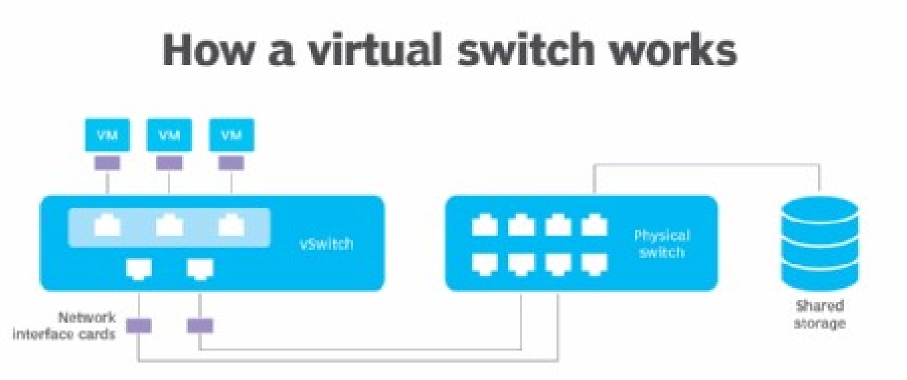


Figure 11: Scheme image about how virtual switches work.

As it can be seen, there is the need to have a physical switch to enable communication between virtual machines and the rest of the network. At the end of the route, there is a shared storage that may be used to be connected to VMware ESXi hosts. [21]

Moreover, virtual switches reduce the complexity of network configurations by decreasing the number of physical switches that would otherwise need to be managed. With additional network and security settings, these switches also provide integrity for VMs.

5.3.1 Types of virtual switches

This subsection will briefly analyze the different types of virtual switches that currently exist. The following table contains the main characteristics of each of them:

External	Internal	Private	Distributed
Uses physical network adapter	Software-defined	Software-defined	Software-defined
Enables the Virtual Machines to access the public network.	Can only access VMs and hosts connected to a similar internal switch.	Can only access VMs connected to a similar private switch.	Extends its ports and management across all servers in a cluster.

Table 4: Different types of virtual switches. [7]

As can be seen in the above table, there are four different types of virtual switches. There is no better or worse among them, which means that using one or another should depend on the characteristics you are looking for when preparing your scenario. Let's now take a deeper look at each one of them:

- **External virtual switches**: This switch type is bound to a physical network card and provides connected VMs with physical external network access. VMs connected to a common external virtual switch can communicate with one another.
- **Internal virtual switches**: Unlike an external virtual switch, an internal virtual switch is not linked to a physical network adapter. Hosts connected to an internal virtual switch can communicate with one another as well as with VMs that are already connected to the internal virtual switch. But VMs connected to an internal virtual switch are unable to connect to the internet or access network resources not connected to the internal virtual switch.
- **Private virtual switches**: A private virtual switch completely isolates the VM. VMs connected to a private virtual switch network can communicate with one another, but they cannot communicate with any resources outside the private virtual switch.
- **Distributed virtual switches**: While standard virtual switches do not extend beyond a single host, distributed virtual switches help to meet the switch demands of clustered virtualized hosts by enabling the cluster nodes to share the same switch across nodes.

5.4 Differences between physical, virtual and virtualized switch

Let's now take a look at the most relevant differences between physical, virtual switches and virtualized switches. It must be considered some different features in order to clearly see how different can be one type of switch from the other. [22]

Features	Physical switch	Virtual switch	Virtualized switch
Physical Description	It is a hardware device that enables the communication across a network in order to permit the connection between devices.	Virtual switches like physical switches enable network components, like virtual machines, to communicate between them. In this case, virtual machines act as operating systems that imitate hardware devices.	A virtualized switch is a software component that uses the image of a real physical switch in order to recreate different kind of scenarios. These images are used in emulator and simulator tools.
Connectivity	The hardware device's network port is connected and physically linked to a point associated with the switching terminal.	A virtualized network adapter is linked to the switch. A hypervisor is used to create virtual switches, allowing a single piece of Information Technology equipment to host multiple VMs.	The connectivity works the same way as if it was a physical switch, which means it will only depend on the case scenario that it is used in.
Configuration Flexibility	On demand flexibility is almost impossible for physical switches. In that case, a manual addition of switches would be required.	Flexibility on configuration can easily be accomplished by simply editing the virtual switch properties.	In this case, virtualized switch have flexibility on configuration due to the possibility to manage its properties depending on the switch image that you are using.
Network Traffic Flow	Network traffic may switch between physical hosts in the same host.	It is not feasible for the network traffic to flow from one virtual switch to another within the same host.	Network traffic works the same way as it was a physical switch. It only depends on the network infrastructure characteristics.
Intelligence	Reviewing the data inside of each frame that goes through the switch is not viable before forwarding them. In order to do that another network device should do it.	As a difference from physical switches, virtual switches have the designed intelligence to review each and every data frame before forwarding them.	Network intelligence does not suit on this kind of switches, another network device should do it.
STP Operations	STP Operations can be done among the switches by exchanging Bridge Protocl Data Unit messages between them. However, those switches have to agree on the root bridge.	STP Operations are not required for virtual switches, as it is not possible to interconnect many virtual switches. As a consequence, the network cannot be configured in order to introduce loops.	They work exactly the same way as physical switches.
Operational Efficiency	Operational efficiency is directly related to the physical hosts. Manual reconfiguration might be required in order to increase the efficiency.	Virtual switches can enhance operational efficiency, boost communications and scale up the system bandwidth because they can aid with migration of virtual devices across the physical host by simply avoiding the requirement of reconfiguration.	The operational efficiency will depend on the case scenario where the virtualized switch is being placed.

Table 5: This table shows the main differences physical and virtual switches.[8]

It is clear that they are not the same and that they have different strengths and weaknesses. However, virtualized switches are kind of a combination between the two main different types of switches. They are specially used in different network emulation/simulation tools in order to recreate real life network infrastructure scenarios.

5.5 Conclusions

From my point of view, it is obvious after all that has been seen that physical and virtual switches are very similar network devices. As a fact, the function that they accomplish is pretty much the same, as they mainly have the labor to interconnect different devices across a network infrastructure.

There is no better or worse between physical and virtual switches, but what is true is that virtual switches have better characteristics as they can be easily modified if needed and they give more bandwidth. Moreover, they are similar to physical switches in being isolated, which thwarts virtual machines from sharing resources with each other.

At the very end, the decision of choosing between one or another depends on the system configuration and whether it is conducive merely to hardware switch terminals or could be expanded to virtual switch contours. We have to take into consideration that virtual switches work for virtual machines, which means that some network infrastructures would not fit this requirement.

Having said all that, it is clear that the IT world is growing day to day and in the near future this kind of network devices will definitely improve their capabilities, as they will have to adapt to the newest technologies. Furthermore, network security is one of the most important aspects when creating, maintaining and repairing network infrastructures as cyberattacks are increasing and adapting to security systems that most businesses have in their private network.

6 Network virtualization

At this point of the project, it has been seen the differences between physical and virtual switches, as well as some of the most relevant characteristics about emulation platforms, but what are really the advantages of using these kind of virtualized environments and devices?

This subsection will be dealing with the advantages of network virtualization, which refers to abstracting network resources that were traditionally delivered in hardware to software.

6.1 Introduction

Network virtualization decouples network services from the underlying hardware and allows virtual provisioning of an entire network. It makes it possible to programmatically create, provision, and manage networks all in software, while continuing to leverage the underlying physical network as the packet-forwarding backplane.

Network and security services in software are distributed to a virtual layer (hypervisors, in the data center) and "attached" to individual workloads, such as your virtual machines (VMs) or containers, in accordance with networking and security policies defined for each connected application. When a workload is moved to another host, network services and security policies move with it. And when new workloads are created to scale an application, necessary policies are dynamically applied to these new workloads, providing greater policy consistency and network agility.

Moreover, virtual networking enables devices across many locations to function with the same capabilities as a traditional physical network. This allows for data centers to stretch across different physical locations and gives network administrators new and more efficient options, like the ability to easily modify the network as needs change, without having to switch out or buy more hardware; greater flexibility in provisioning the network to specific needs and applications; and the capacity to move workloads across the network infrastructure without compromising service, security, and availability. [23]

6.2 Benefits and advantages

Virtual networking delivers a variety of business benefits, from lowering capital expenditures and maintenance costs to easily segmenting networks. Specifically, a virtual network:

- Streamlines the amount of network hardware (cabling, switches, etc.) by shifting many functions to software.
- Reduces the cost and complexity of managing network hardware and software through centralized control.
- Offers more flexible options for network routing structure and configuration, including easier options for segmenting and subdividing the network.
- Improves control over network traffic with more fine-grained options, like configuring firewalls at the virtual NIC level.

- Increases IT productivity through remote and automated service activation and performance testing.
- Boosts business scalability and flexibility by enabling virtual upgrades, automated configuring, and modular changes to network appliances and applications.

In addition, network virtualization helps organizations achieve major advances in speed, agility, and security by automating and simplifying many of the processes that go into running a data center network and managing networking and security in the cloud. Here are some of the key benefits of network virtualization:

- Reduce network provisioning time from weeks to minutes.
- Achieve greater operational efficiency by automating manual processes.
- Place and move workloads independently of physical topology.
- Improve network security within the data center.

6.2.1 Virtual servers

Server virtualization implementations have proliferated because the benefits of virtualization are extensive and can be realized quickly. Some of their most relevant advantages are: [24]

- With virtualization, the less-demanding Operating Systems and applications can run on a single machine, thus saving server hardware costs. The net effect is that fewer servers are required because they are being used more efficiently.
- Server virtualization provides an easy way to provision specific resources to individual servers and their applications.
- New servers can be spun up and deployed quickly without requiring a lot of time. When a server is no longer needed, it can easily be decommissioned and taken down.
- Server virtualization systems have centralized management applications where the status of all virtual servers can be monitored and adjusted as needed.
- Virtual servers can be moved or cloned from one piece of hardware to another, making hardware upgrades and performance tuning a nearly effortless process.
- Hosting multiple Operating Systems in one single server hardware device.
- When a disaster disables a data center, virtual servers can be quickly spun up at a remote site to enable business processes to continue.

Although this virtualization has many advantages, it also has some potential disadvantages. Running multiple virtual machines on one physical machine can result in unstable performance if infrastructure requirements are not met.

Moreover, virtual machines are less efficient and run slower than a full physical computer. Most enterprises use a combination of physical and virtual infrastructure to balance the corresponding advantages and disadvantages.

6.2.2 Virtual switches

Virtual switches have clear advantages over physical switches. The fact that they are software devices reduces the time spent when connecting them to a network infrastructure. For example, when a physical switch is connected to a network infrastructure, there is the requirement to plug all the cables, find the necessary space where to put it as well as to make the necessary configuration to make it run on the existing network infrastructure.

The time spent for this implementation is quite elevated, whereas for virtual switches the only thing that you have to do is to get the device's firmware, upload it to the virtualized environment and configure it. Even the configuration would not be necessary in some occasions, as there is the possibility to upload pre-made configurations on such devices. As a fact, the time that someone would spend on connecting a virtual switch would be clearly reduced in comparison to connecting a physical one.

Moreover, the hardware device cost is elevated, as manufacturers fix its price based on the physical structure itself as well as the necessary firmware to make it run. On the other hand, for virtualized switches the only requirements are to have the appropriate virtualized environment to run them and the manufacturers firmware. It is a clear indicator that with virtual switches a lot of money can be saved.

Last but not least, virtual switches are designed with the sufficient intelligence to review each and every data frame before forwarding them, increasing in that way the ability to monitor and control all the data that goes trough a network, and benefiting the detection of possible threads and intrusions.

6.3 Conclusions

To conclude, it is clear that virtual networking is getting more and more influence as the time goes by. The benefits from virtualizing a network infrastructure and its devices is ridiculously big, not only because you save time and money but also because the maintenance and management of the different network devices is easily carried out through centralized control, as well as it offers more flexibility options for network routing structure and configuration.

Moreover, network virtualization is rewriting the rules for the way services are delivered. This approach moves networks from static, inflexible, and inefficient to dynamic, agile, and optimized.

Last but not least, network virtualization can offer a virtual environment for not only business optimization and scalability but for educational purposes and security testing, as it provides unlimited riskless scenarios.

7 Experiments and results

In this section, an explanation of the procedure followed for the configuration of one of the laboratories previously designed will take place. This configuration will be done as if one of the students had to complete the lab practice, in order to show the results of how a practiced should be completed, as well as to rate the difficulty of it and point out the skills that will be achieved. The next image shows the scenario that has to be configured:

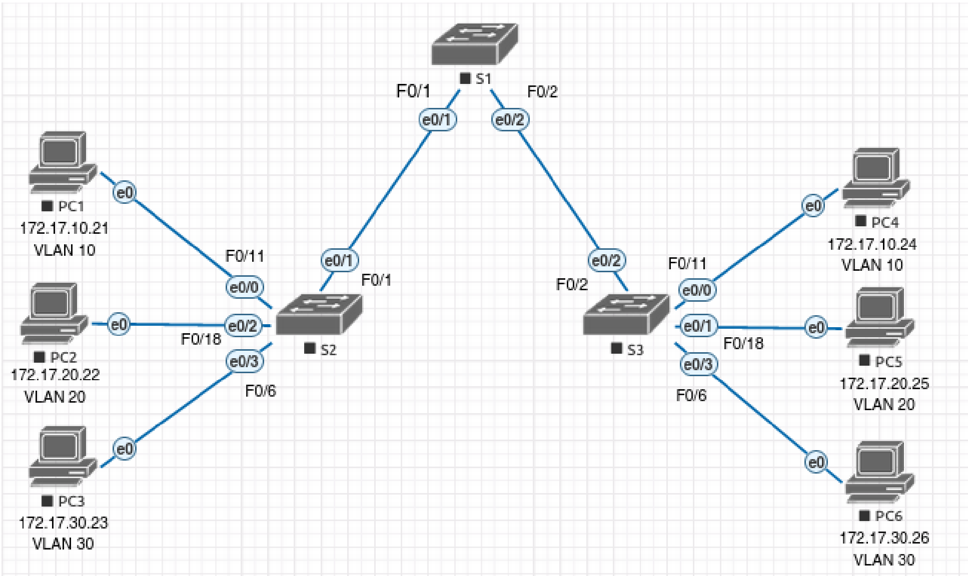


Figure 12: Lab 3.5.1: Basic VLAN Configuration

As it can be seen, this scenario shows three different switches; S1, S2 and S3. The main switch, S2, is directly connected to S1 and S3; this way, the endpoints that are connected to S2 can have communication with the endpoints connected to S3, so S1 will be acting as a bridge between these two sub-networks of the designed infrastructure.

Each created scenario will have to be done following some predefined configuration and tasks that will be given by the teacher during the laboratories hours. This initial information is the different IP's that each device has plus the initial port assignments (Note that although the nomenclature of Fast Ethernet is given, with an 'F' followed by the interface, on the practice we will be using normal Ethernet instead, with an 'e' followed by the interface). Here is an image of the predefined configuration that has just been mentioned:

Addressing Table

Device (Hostname)	Interface	IP Address	Subnet Mask	Default Gateway
S1	VLAN 99	172.17.99.11	255.255.255.0	N/A
S2	VLAN 99	172.17.99.12	255.255.255.0	N/A
S3	VLAN 99	172.17.99.13	255.255.255.0	N/A
PC1	NIC	172.17.10.21	255.255.255.0	172.17.10.1
PC2	NIC	172.17.20.22	255.255.255.0	172.17.20.1
PC3	NIC	172.17.30.23	255.255.255.0	172.17.30.1
PC4	NIC	172.17.10.24	255.255.255.0	172.17.10.1
PC5	NIC	172.17.20.25	255.255.255.0	172.17.20.1
PC6	NIC	172.17.30.26	255.255.255.0	172.17.30.1

Initial Port Assignments (Switches 2 and 3)

Ports	Assignment	Network
Fa0/1 – 0/5	802.1q Trunks (Native VLAN 99)	172.17.99.0 /24
Fa0/6 – 0/10	VLAN 30 – Guest (Default)	172.17.30.0 /24
Fa0/11 – 0/17	VLAN 10 – Faculty/Staff	172.17.10.0 /24
Fa0/18 – 0/24	VLAN 20 – Students	172.17.20.0 /24

Figure 13: Information about the predefined configuration of the scenario.

7.1 Initial configuration

First of all, we have to set up all this initial configuration. In order to create each VLAN interface, we have to do the following on each of the switches respectively (I will be showing how the S2 should be configured with its IP):

- We open the switch terminal and then we input the following command to enter into *EXEC mode* ***enable***.
- Next, we have to enter into the configuration terminal by typing ***config term***.
- By introducing the command ***interface vlan 99*** the VLAN will be created.
- Afterwards, we give him the corresponding IP address by typing ***ip address 172.17.99.12 255.255.255.0***.
- By typing ***show vlan brief*** we can check if the VLAN has been successfully created.
- In order to correctly assign the PC's initial configuration, we have to start the PC, go to *Control Panel*, then to *Network and Internet*, then click on *Network and Sharing Center*, then click on *Change Adapter Settings*, next click on *Local Area Connections*, open its *Properties*, click on *Internet Protocol Version (TCP/IPv4)* and manually introduce the respective IP address, its Subnet Mask and the IP address of the Default Gateway.

After this, the initial port assignments must be configured. In order to do so, the following has to be done:

- First of all, TRUNK mode on VLAN 99 has to be switched. In order to so, we have to enter into the configuration of the VLAN and type ***switchport mode trunk***.
- Next, ports Fa0/1 - 0/5 have to be assigned to VLAN 99. This will be accomplished by entering into the *EXEC mode*, then go to the configuration terminal, then get into VLAN 99 by typing ***vlan 99***, then we select the range of interfaces by typing ***interface range e0/0-5*** and ***switchport trunk vlan 99***. Afterwards, the whole range has to be selected again and the following command ***no shutdown*** has to be executed.
- The next step is to create the VLAN 30, VLAN 10 and VLAN 20, the same way the VLAN 99 has been created, and assign the corresponding ports to these VLANs.

The scenario configuration that must be done is divided into two main tasks. These tasks are the following:

Task 1: Prepare the Network

Step 1: Cable a network that is similar to the one in the topology diagram.

You can use any current switch in your lab as long as it has the required interfaces shown in the topology.

Note: If you use 2900 or 2950 switches, the outputs may appear different. Also, certain commands may be different or unavailable.

Step 2: Clear any existing configurations on the switches, and initialize all ports in the shutdown state.

If necessary, refer to Lab 2.5.1, Appendix 1, for the procedure to clear switch configurations.

It is a good practice to disable any unused ports on the switches by putting them in shutdown. Disable all ports on the switches:

```
Switch#config term
Switch(config)#interface range fa0/1-24
Switch(config-if-range)#shutdown
Switch(config-if-range)#interface range gi0/1-2
Switch(config-if-range)#shutdown
```

(a) Task 1

Task 2: Perform Basic Switch Configurations

Step 1: Configure the switches according to the following guidelines.

- Configure the switch hostname.
- Disable DNS lookup.
- Configure an EXEC mode password of **class**.
- Configure a password of **cisco** for console connections.
- Configure a password of **cisco** for vty connections.

Step 2: Re-enable the user ports on S2 and S3.

```
S2(config)#interface range fa0/6, fa0/11, fa0/18
S2(config-if-range)#switchport mode access
```

(b) Task 2

Figure 14: Three different scenarios.

Once all the previous configuration has been done, it is time to begin with the tasks that have to be done in order to complete the practice. The same configuration for each one of the switches will be shown, taking into consideration the different interfaces of each one of them. Let's take a look of how should be done in the case of S2. There is a list of switch commands that Cisco provides in its own official web page that can be used in case that some help is needed. [25].

7.2 Tasks

7.3 Task 1 - Step 1

This first step is already done, as it is only to cable the scenario using the EVE-NG emulator tool. It has to be considered that each switch is using a Cisco IOL image, where IOL reefers to the used Linux version and each endpoint are using Windows O.S. The switch image is defined as *L2-ADVENTERPRISEK9-M-15.2.bin* in the platform repository.

7.3.1 Task 1 - Step 2

To begin with Step 2, all the previous configurations have to be cleaned from the switch. In order to do so, the first step is to open the switch terminal by running the switch and left-clicking on it. Once the access to the terminal is achieved, it is mandatory to enter into *EXEC mode*, in order to have the right privileges to modify its configuration. This will be achieved by typing ***enable***.

Before cleaning up its configuration, it is recommended to check up any configuration on the switch. By typing ***show running-config***, all the configuration will be shown in the terminal. If there is any startup configuration running, it must be deleted by introducing the command ***delete startup-config***. If then the switch is rebooted, the configuration that will be running will be the default one, which was what we were looking for.

Afterwards, *EXEC mode* must be accessed and then, by typing ***config term*** it will be possible to access to the configuration of the terminal. Next, all the interfaces that are being used in the case scenario have to closed by typing ***interface range e0/1-3*** and then executing the command ***shutdown***.

7.3.2 Task 2 - Step 1

This second task begins with some basic switch configuration, as can be seen in Figure 7 (b), five small tasks have to be completed. These are achieved by doing the following:

- **Configure the switch hostname**. It is mandatory to enter into *EXEC mode*, then type ***config term*** to be able to modify the switch configuration. After it, by just typing ***hostname S2*** the hostname of the switch will be automatically changed from Switch to S2.
- **Disable DNS lookup**. Again, it is necessary to type ***enable*** to enter on *EXEC mode* and ***config term*** to gain access to the switch configuration terminal. By just typing ***no ip domain-lookup*** the DNS lookup will be disabled.
- **Configure an *EXEC mode* password of *class***. Now, a configuration of a password for entering into *EXEC mode* has to be established. This will be achieved by typing ***enable password class*** on the configuration terminal mode.
- **Configure a password of *cisco* for console connections**. On *EXEC mode*, once you get access to the configuration terminal, the command ***line console 0*** has to be typed and then type ***password cisco*** in order to modify the password. The *console 0* term is to connect a swtich / router through medium console. If there is only one console port, you can only choose "line console 0".
- **Configure a password of *cisco* for vty connections**. Before configuring the password, the number of vty lines must be checked. This can be accomplished by introducing the command ***line vty ?***. In this case, there are four vty lines. Afterwards, on *EXEC mode* and having accessed to the configuration terminal, the command ***line vty 0 4*** has to be introduced. Consider the VTY 0 4 as the door of entry to the router. With the "login" command you are basically locking the door. The password is the key to open the door.

7.4 Task 2 - Step 2

In order to complete the second step of the task 2, it is necessary to re-enable the user ports on S2 and S3. In order to do so, these steps will help to get to it:

1. Go on *EXEC mode* and type the corresponding password (*class*).
2. Get into the configuration terminal by typing ***config term***.
3. Now select the range of interfaces that have to be re-enabled *interface range e0/0, e0/2, e0/3*.
4. Last but not least, it is necessary to change the *switchport* mode in order to turn on the access mode. There are three different types of *switchport* modes, which are ACCESS, TRUNK and LOCAL. By executing the command ***switchport mode access*** ACCESS mode will be selected. Then, by typing ***no shutdown*** all selected ports will be re-enabled.

After this last step, the lab practice would be completed. The write up that has been done can be used as a report to hand in to the professor that evaluates it. The only missing information would be the configuration that has been carried out on each of the switches. The scenario that has been configured is part of easy difficulty scenarios, as the configuration of the scenario is really basic, taking into consideration that the students that will be resolving this case scenarios already have a big background on switch configuration. Moreover, the time that an advanced student would spend on the resolution is approximately of 10 minutes, which clearly indicates the ease when resolving it.

The skills that the student will achieve after completing the configuration of this network infrastructure scenario are the following:

1. Cable a network according to the topology diagram.
2. Erase the startup configuration and reload a switch to the default state.
3. Perform basic configuration and tasks on a switch.
4. Create VLANs.
5. Assign switch ports to a VLAN.
6. Add, move and change ports.
7. Verify VLAN configuration.
8. Enable trunking on inter-switch connections.
9. Verify trunk configuration.
10. Save the VLAN configuration.

8 Budget

Depending on the thesis scope this document should include: This section will deal with the total cost of project development. In order to carry it out, the main expense is the student who develops it and the teachers/supervisors from both universities.

In our case, one supervisor of the CTU and one tutor from UPC were involved. To fulfill the 18 credits of the thesis, is expected to dedicate about 25 hours/credit, thus approximating a total of 450 hours. The CTU supervisor attended, approximately in total, 1h every two weeks, resulting in a total of 9 weeks. Counting extra work for the evaluation, about 14 hours of work are considered to be directly dedicated to this project. With the UPC tutor, as there is no continuous weekly evaluation, approximately 8 hours of work are estimated, taking into account coordination and evaluation. The total budget is 5832€ as we can see in the following table.

	Number	Salary (€/hour)	Hours	Salary (€)	Taxes (21%)	Total (€)
Student	1	9	450	4050	850	4900
CTU Supervisor	1	35	14	490	103	593
UPC Supervisor	1	35	8	280	339	339
BUDGET						5832

Table 6: Table showing the budget considered during the development of the Thesis.

For the materials part, we must take into account the computer and the server where the data is stored, as the student was offered to work completely remotely there is no need to include an office space for the development of the Thesis. Considering the computer of the student is 1.300€, with a life expectancy of 7 years (84 months) and a residual value of the 25 percent . We can calculate the amortizations as:

$$f = \frac{initialTotal - residualValue}{lifeExpectancy}$$

For the server we can approximate the cost to 1.025€, with a life of 120 months and a residual value of a 10 percent. The cost of the materials is as show in the next table, where the use of them is of 5 months.

	Amount	Cost (€)	Initial total (€)	Residual value (€)	Amortization (€)	Total (€)
Computer	1	1500	1500	375	14	70
Server	1	1025	1025	102	8	40

Table 7: Total amortization related to materials.

9 Conclusions

The aim of this thesis was the creation of some different network infrastructure scenarios for new incoming CTU students next semester, and, as a consequence, learn how an emulator tool works, its benefits and deficiencies. Moreover, the virtualization of different network devices such as servers or switches is leading to a whole new meaning for network infrastructure, which is called virtual networking. This concept has been evolving during these last years and it is important to understand it in order to adapt to it.

Thanks to the work that has been carried out, I was capable to learn how to use an emulator platform, from the creation of the different scenarios, that is only the visual part of it, to the configuration of a couple of them, of the different devices that appear on it, as well as testing the configuration itself. Furthermore, the theoretical research about this kind of platforms has brought me more knowledge about this IT sector, about the differences between emulator and simulator platforms, as well as the most important emulation and simulation tools and the benefits that SMEs could have using one or the other.

In addition, the differentiation between physical and virtual switches has brought me to understand the meaning of virtual networking, about virtualizing a network infrastructure and its devices. This project has shown that there are a lot of benefits from virtualizing network hardware devices such as servers and switches, as well as LAN's, not only because it delivers more centralized management and simplified network management but also because the disparate parts of the network can be accessed remotely for needed updates and changes, or even testing, making network management cheaper and easier.

10 Future Work

The only way to continue this work is to test the different lab scenarios that have been designed, in order to find any defect on the creation of them. Moreover, the PDF instructions that are shown before doing the laboratory could be included in the designed scenario so the student could have all the necessary information in order to complete the practice.

References

[1] A. Toynbee. The story of bridging. https://cseweb.ucsd.edu/~varghese/TEACH/cs123/bridging.pdf. Accessed: November 23, 2022.

[2] What is it infrastructure? - the backbone of technology. https://www.matrix-ndi.com/resources/it-infrastructure-hubs-switches-routers, January 27, 2022. Accessed: November 30, 2022.

[3] Unknown. What is the difference between emulators and simulators? https://www.racksolutions.com/news/blog/what-is-the-difference-between-emulator-and-simulator/.

[4] I-Mediata Admin. Top 10 most popular network simulation tools. https://www.imedita.com/blog/top-10-list-of-network-simulation-tools/.

[5] Andrew Froehlich. Managed vs. unmanaged switches: What are the differences? https://rebrand.ly/x6xadnm. Accessed: December 5, 2022.

[6] Gary McCauley. Network switch: Managed vs unmanaged. https://rebrand.ly/31smb7n. Accessed: December 5, 2022.

[7] Alexander S. Gillis. virtual switch (vswitch). https://www.techtarget.com/searchitoperations/definition/virtual-switch. Accessed: November 23, 2022.

[8] Rashmi Bhardwaj. Physical switch vs virtual switch: Which is the best choice? https://networkinterview.com/physical-switch-vs-virtual-switch-which-is-the-best-choice-you-can-go-up-with/. Accessed: November 22, 2022.

[9] Openvpn. https://openvpn.net/community-resources/how-to/.

[10] Openvpn. https://openvpn.net/vpn-client/.

[11] Emulating virtual environment - next generation. https://www.eve-ng.net/index.php/documentation/howtos-video/.

[12] Emulating virtual environment - next generation. https://www.eve-ng.net/index.php/documentation/professional-cookbook/.

[13] Emulating virtual environment - next generation. https://www.eve-ng.net/.

[14] Dominik Ziajka Jeremy Grossmann and Piotr Pekala. Graphical network simulator - 3. https://www.gns3.com/software.

[15] Cisco Systems. Cisco packet tracer. https://www.netacad.com/courses/packet-tracer.

[16] Sally Floyd Tom Henderson, George Riley and Sumit Roy. Network simulator - 3. https://www.nsnam.org/.

[17] Cisco Systems. Cisco virtual internet routing lab. https://learningnetwork.cisco.com/s/virl.

[18] DANIEL LIBERTO. Small and mid-size enterprise (sme) defined: Types around the world. t.ly/c88AV.

[19] Techopedia. Switch. https://www.investopedia.com/terms/s/smallandmidsizeenterprises.asp. Accessed: November 7, 2022.

[20] Moumita. What are switches in computer network? https://www.tutorialspoint.com/what-are-switches-in-computer-network. Accessed: November 22, 2022.

[21] VMware. Vmware virtual networking concepts. https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/techpaper/virtual_networking_concepts.pdf. Accessed: November 22, 2022.

[22] Nathan Cranford. Physical switches vs. virtual switches. https://www.rcrwireless.com/20180328/fundamentals/physical-switches-vs-virtual-switches. Accessed: November 22, 2022.

[23] VMware. Vhat is virtual networking? https://www.vmware.com/topics/glossary/content/virtual-networking.html. Accessed: January 10, 2023.

[24] Rich Castagna. 10 benefits of server virtualization for businesses. https://www.techtarget.com/searchitoperations/tip/10-benefits-of-server-virtualization-for-businesses. Accessed: January 10, 2023.

[25] Cisco Community. Switching. https://community.cisco.com/t5/switching/bd-p/6016-discussions-lan-switching-routing. Accessed: December 30, 2023.