Towards a virtualized Internet for computer networking assignments

Luis Bellido, David Fernández, Encarna Pastor

Abstract— **By combining virtualization technologies, virtual private network techniques and parameterization of network scenarios it is possible to enhance a networking laboratory, typically carried out in university laboratory premises using equipment located there, by interconnecting it to virtual networks running on the students' own personal computers. This paper describes some experiences applying this model to create hands-on assignments for a large group of students in computer networking education.**

Computer networks; parametrized exercises; virtualization; LMS

I. INTRODUCTION

The use of virtualization technologies in educational computer networking laboratories can significantly help to reduce equipment costs and work effort. Some of the elements of a networking laboratory scenario can be virtualized (i.e., implemented using virtual machines) over shared servers able to host even tens of these systems. This paper describes proposals and experiences in which the virtualization of the network laboratory is extended to the students' own personal computers.

From the pedagogical point of view, student interactions with a networking laboratory environment are practically the same as the interactions they would have with a real network. The authors have used virtual network scenarios, using VNX[1] as the virtualization tool, to create hands-on assignments for "Computer Networks" subjects. VNX allows specifying in a simple way network scenarios composed of virtual machines interconnected in a topology defined by the user. By parameterizing the definition of the virtual network scenario, each student can be assigned an individual personalized network, which is different from those of the rest of the students. This has proven to be useful in an academic context where the number of students in a semester can be in the range from 100 to 400 depending on the subject and the year. Students can choose to do their personalized assignment using a computer in the laboratory where the VNX environment is installed. But it is also possible for the students to download a virtual machine image including VNX, that can be run on generic virtualization software such as Virtual Box or, if they already have a Linux box, to install VNX on their own machine.

In the first semester of the current academic year 2012/13, the authors have prepared a new assignment based on a distributed virtual network scenario in which a personalized network scenario, running on the student's own personal computer, is connected to a central network scenario based on a combination of virtualized and real network components on the laboratory premises. The assignment will allow students to better understand the routing protocols used on Internet, specifically the interdomain routing protocol BGP and the intradomain routing protocol OSPF. Students will configure and analyze the OSPF protocol on a virtual network scenario running on their local machine. Then they will connect their virtual network scenario, representing an Autonomous System on the Internet, to the laboratory central scenario, representing the Internet backbone, and they will be able to configure and analyze the BGP protocol.

This paper discusses the technologies used to create this assignment, i.e. virtualization technologies, virtual private network techniques and integration of the assignment on a Learning Management System (LMS). It will report on the results of this work from three different perspectives: the laboratory infrastructure perspective, the teacher perspective and the student perspective.

From the laboratory perspective, the paper provides an overview of the infrastructure required to support this kind of assignments and reports on how this first edition of this "virtualized Internet" assignment worked in practice.

From the teacher perspective, the paper first explains the process of design of this kind of assignments, and then it reports on different tasks supporting the assignment, such as student support through on-line forums and in the classroom, or evaluation of student results.

From the student perspective, the paper analyses the impact on the students learning and workload, using data collected from on-line questionnaires, personal interviews and also the results of the evaluation of the assignment and the final test for the subject.

[1] Virtual Networks over linuX (VNX), http://www.dit.upm.es/vnx.

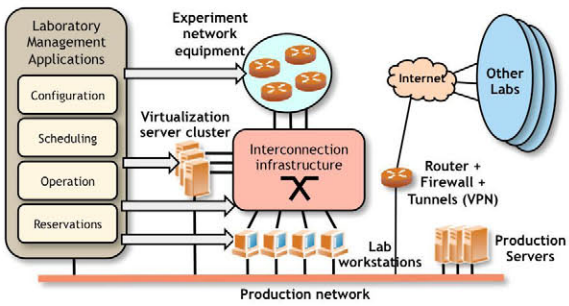

Figure 1. Virtual network laboratory model

II. VIRTUAL NETWORK EXPERIMENTS FOR ENGINEERS

A. Academic context

The authors have used virtual network experiments for several years in the course "Computer Networks". The number of students matriculated in this course in different years has been from around 100 to more than 300. The first time an experiment of this kind was introduced in this subject, in academic year 2007/08, it was proposed as a voluntary task that the students could carry out as an alternative to an exercise "on paper". Out of the 318 students that handed-in the results for this task, only 29 (9 %) chose the practical experiment. However, the experience was very positive, both because it worked without any problems and because the good feedback we received from the students that carried it out. So the next year the experiment substituted the exercise on paper completely.

This year 2012/12, the course "Computer Networks" has been adapted to the new organization of university degrees in Spain, in the framework of the Bologna process in Europe. In this context, the use of "hand-on" experiments to support the learning process of the future engineers is even more important and has been one of the motivations to increase the use of virtual network experiments.

B. Laboratory infrastructure (model)

This section describes a computer network laboratory model based on distributed virtualization. The requirements of this model are the result of experience acquired during several years of use of virtualization scenarios tools in the teaching laboratories on the DIT-UPM network.

The most relevant elements of the physical network infrastructure are shown in Figure 1.

Production network: it provides basic connectivity of the laboratory for access to user accounts, Internet, and laboratory management consoles. This network is not used for experimentation practices.

Interconnection infrastructure: it is the basis of the experimental network, facilitating the interconnection of the real and virtualized elements that are part of the practice scenarios. This infrastructure allows the definition of multiple networks through the use of virtual LANs (VLAN). This infrastructure is managed from the production network.

Virtualization servers: computers that support one or more virtualization technologies and that are capable of hosting virtual machines to be used in different practice scenarios.

Laboratory workstations: personal computers where users (students) do their usual activities. They are provided with two network interfaces: one connecting to the production network and the other one connecting to the experimental network infrastructure.

Physical laboratory equipment: various types of physical equipment (routers, terminal servers, and so on) that will be part of the practice scenarios.

Laboratory management: a set of tools to manage the virtualization supported computer network laboratory.

Lab router: is the element connecting the lab to Internet. The firewall functionality is included for security reasons, while the tunnel functionality is used to establish channels of communication with machines (physical and / or virtual) from other remote venues.

Other laboratories: this represents the possibility to define practice scenarios involving elements that can be located in other laboratories with similar characteristics.

The objective of this laboratory model in the context of teaching telecommunication engineers is to support laboratory practices based on complex scenarios. For the first time, this laboratory is used to support an experiment where the practice scenario is distributed among the central laboratory and the student personal computers.

C. Student controlled virtual scenarios

The specification of virtual network scenarios for laboratory experiments, especially those involving a mix of real specific physical machines and virtual machines, is usually reserved for teachers or administrators of the laboratory. However, in some of the experiments, it is desirable that students can access the laboratory to run simple scenarios, for example to analyze the behavior of a particular network protocol. In this case, the scenario might require just a single host with virtualization support. Sometimes, the scenarios created by a student can also be integrated into a more general setting that includes other scenarios specified and controlled by other students or by teachers.

This functionality can be achieved by giving the students a controlled set of user rights in some of the virtualization servers, so that they can define and start virtual scenarios. A more flexible option is that the lab workstations have also the capability of running virtualized network scenarios, so the students can define and run their virtual scenarios on their local machines at the laboratory. This can be restricted to scenarios that just run on the local host without external communications, or to specific scenarios that will be integrated with other scenarios running externally. This option is already available at DIT laboratories and has been used successfully in several practices.

D. Parameterized virtual scenarios

As a special case of student controlled virtual scenarios, some theoretical subjects are using virtual scenarios as a way to

provide practical networking experiments for their students. In this case, an important factor to take into account is the high number of students that can take these subjects in a semester, from 100 to more than 300 depending on the subject and the year. In this context, it is convenient to use parameterized experiments, in which there is a common description of the problem for all students, but a different set of parameters for the experiment of each student [1].

For parameterized virtual scenarios, the process of parameterization is done beforehand, so each student receives a different virtual network configuration file. For the OSPF routing exercise, each student receives a different VNX file describing a network with two hosts and five routers as shown in Figure 2. The parameterized values in this case are the IP addresses, and the routing protocol link costs for each of the links interconnecting the routers, so each student will get different results when they perform the different tasks defined in the exercise, such as analyzing the OSPF routing information database of a router or running a traceroute between two hosts.

This kind of scenarios are normally designed to minimize the hardware requirements, so it is not only possible to run the virtual scenarios at one of the lab workstations, but it is also possible for the students to download the whole environment needed to run a virtual scenario on their own personal computer. For example, it is possible to create a Live Linux distribution that the students can download with all the tools needed to run the virtual network. It is also possible to run the virtual network scenario inside a virtual machine. Using this option, instead of downloading a Live Linux distribution, students can download a virtual machine image that can be opened in a virtualization software package, such as Oracle VM VirtualBox [2]. However, it would also be interesting to give access to students to the virtual network scenarios from their own personal computers without the need of downloading a live distribution or a virtual machine image. Ideally, it should be possible to access the network scenarios from a web browser as discussed in [3].

III. ROUTING EXPERIMENT

A. Requirements

In order to improve the teaching-learning process in the area of routing protocols for IP networks, an experiment has been designed that allows students to interact with a network scenario composed of different Autonomous Systems (AS) interconnected hierarchically. The main objective is to allow the students to apply the routing protocol concepts learnt in class about the OSPF and BGP protocols using real implementations, as well as getting some practical skills about the configuration and management of IP networks.

The academic context of the Computer Networks course, mainly the number of students and the resources available, led the authors to identify the following main requirements for the experiment:

- It should be possible to carry it out using a standard personal computer (preferably owned by the students) with an Internet connection.

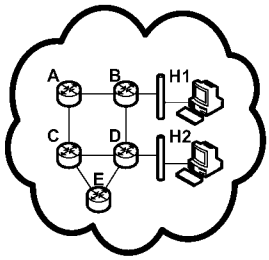

Figure 2. Student network topology

- It should not require the students to install any complex programs or new operating systems on their computers.
- It should not require any knowledge of the emulation tools used to create the network scenario.
- It should allow the students to interact with real OSPF and BGP implementations and to capture network traffic using standard tools like Wireshark.
- It should be possible to correct automatically most of the questions asked in the exercise.
- The exercise should be basically the same for every student, but the data (IP addresses, link costs, etc.) has to be personalized so every student has to solve it individually.

With all these requirements in mind, the designed solution has two components: a central network scenario running on the laboratory premises, and a set of network scenarios that will run on the students' personal computers. Each student network is an Autonomous System composed of several nodes (routers) and end-systems (hosts) that will be connected to one of the routers in the central network scenario. The student networks are implemented using the VNX tool, which will be run inside a VirtualBox virtual machine that contains all the tools needed to run the virtual network and to connect it to the central networks scenario.

B. Experiment description

To carry out the exercise, the students have to download and install the Oracle VM VirtualBox software and then the VirtualBox image that has been prepared for the experiment. Once the students have started the virtual machine, they have to download a ZIP file from the subject moodle server containing their personalized scenario and some scripts to start and stop the network scenario.

Figure 2 shows the student AS network topology, made of five routers running OSPF protocol and two hosts. The scenario is initially started with everything correctly configured. The students do not know the topology of the network: they just know that there are five routers and two hosts (all of them Linux systems) and they have access to their consoles. The first task they have to carry out is to discover the topology of the network by using "ping" and "traceroute" tools, as well as consulting the information obtained through system consoles. They have to draw a complete map of the network that they provide as a result of the exercise.

Later they have to shutdown one of the network links to see how the traffic is automatically rerouted though the alternative path. Besides, they have to capture the packets interchanged by routers using the Wireshark protocol analyzer, in order to understand how OSPF protocol works.

Once the students have finished testing and analyzing the OSPF protocol, they will connect their virtual network scenario, representing an Autonomous System on the Internet, to one of the ISPs at the laboratory central scenario, using a VPN connection (Figure 3). After checking the IP connectivity between their network and the BGP router at the ISP, they will configure their edge router so the BGP session is established. Then, by looking at the routing information on a "looking glass" (LG) they will check how the routing information is propagated from their AS to the rest of the network. The students will capture and analyze the BGP traffic exchanged between their AS and the ISP and they will be able to verify how the routing tables change when there is a change in the network, such as a link shutting down.

Apart from the network map and the answers to the questions posed, the students have to submit a Wireshark capture file containing the traffic captured on the experiment scenario. These files are later processed with ad-hoc scripts to check that they contain the packets interchanged by routers during the link failure event and that the addresses found in the capture file correspond to the addresses assigned to each student. In this way, it can be easily checked that the students have made the exercise using the data assigned to them.

IV. Experiment Design and Implementation

A. *Laboratory perspective*

From the point of view of laboratory infrastructures, this kind of practical exercises demand a stable and relatively powerful infrastructure to support all the virtual machines that are part of the central and auxiliary virtual scenarios. Besides, a good Internet connectivity and a VPN service are needed to connect the student virtual scenarios to the core network.

Basically, the laboratory infrastructure has to support the central virtual scenario that resembles the Internet core of autonomous systems interconnected either directly or through Internet exchange points (IX). This backbone scenario is made of around 20 virtual machines that act as network routers or support servers. Besides, as the students are requested to test connectivity with other client networks (some *traceroute* and *ping* tests have to be provided as a result) and the exercise is available with an open timetable, some always-available reference client networks have to be deployed to allow the students to perform tests. These client virtual networks add around 40 new virtual machines, which together with some other systems used for monitoring and other auxiliary services made a final requirement of near 70 virtual machines.

To support the experiment, a server with the following characteristics has been used: Sun Fire X4150 with dual Xeon E5440 CPU at 2.83GHz and 16 GB of RAM running Ubuntu 12.04 operating system and with VNX installed. This server is completely dedicated to the exercise during the experiment period.

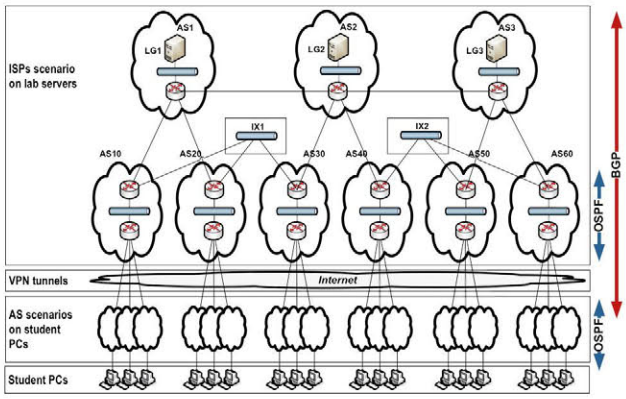

Figure 3. OSPF/BGP experiment complete topology

To provide the needed connectivity between student and central scenarios, a solution based on the free software *tinc* [4] has been used. *tinc* is a Virtual Private Network (VPN) daemon that uses tunnelling and encryption to create a secure private network between hosts on the Internet. It is available in most Linux distributions and has proved stable and scalable enough to support the experiment. For the connectivity, the standard university Internet connection has been used, as the traffic generated by the exercise is very low: the students only generate some test traffic (ping, traceroute and web access to monitoring tools).

For those students not having a computer or Internet connection available, we offer the possibility to carry out the exercises at the university laboratories. In this case, the connectivity among the student scenarios and the core is made directly though the laboratory switches using VLANs, not needing to use the tinc VPN solution described above.

One of the main concerns related to the infrastructure supporting the exercise is the stability of the whole environment. To give flexibility, the students are allowed to connect to the central scenario at any time, although troubleshooting support is only provided during working hours. Besides guaranteeing that the equipment and services involved are stable, the supporting staff has also to cope with the possible instabilities caused by student's misconfiguration errors. As the students interact directly with the basic routing protocol of the network, its errors can cause connectivity problems to other students.

Therefore, a solid monitoring system has to be built around the exercise in order to promptly detect problems either in the equipment used or in the configuration of student's scenarios. Two basic active systems are used for monitoring purposes: a *nagios* system [5] that continuously checks the network connectivity among all the staff controlled systems, as well as the connectivity to student scenarios; and a *BGPmon* [6] system that monitors and records the BGP routing table.

Apart from guaranteeing the stability of the exercise environment, the monitoring systems, together with other log traces (for example, the ones generated by tinc), can be used to evaluate the activity of the students, giving interesting

information about the time invested for carrying out the exercise, the main mistakes made, and so on.

B. Teacher perspective

In this kind of experiment, the teacher creating it will need to write a generic set of instructions and questions for the students that can be answered by running the parameterized experiment. In order to support the distribution of a specific network scenario for each student, the collection of student answers and the delivery of evaluation results, a set of generic open tools have been designed and developed, targeting subjects with an elevated number of students. These tools, integrated in a Learning Management System, aid in the creation and publishing on the web of personalized exercises, provide online forms for the students to hand in their answers, and facilitate the evaluation and publishing of the grades by the teachers and the evaluation of the impact of these exercises in the learning process.

Figure 4 shows how a personalized virtual network exercise is developed and carried out, highlighting the components that are related to the virtual network parametrization.

For personalized virtual networks, the personalization component consists of a set of virtual network configuration files that the student will retrieve from the assignment tool. The student will use these files to run the virtual network scenario using the generic virtual network environment (VNX). A teacher will create these configuration files using a set of configuration creation scripts that will need to be developed ad-hoc depending on the actual network scenario.

For the OSPF/BGP routing exercise, the process of creating the personalized virtual network configuration files is as follows. From the initial network scenario, some of the parameters of the scenario are selected for personalization, in this case the IP addresses, the costs of the links and the address of the central network scenario router to which the student AS will connect. Using a spreadsheet the teacher compiles all the personalized values. The spreadsheet is then converted to an XML parameter values file that will be used to feed the configuration creation scripts. On the other hand, the initial virtual network scenario is created and tested using VNX. The configuration file in XML is then used as the basis for an XSLT file that facilitates the creation of the different virtual network description files using the XML parameter values files. This solution, based on XSLT, also allows the creation of configuration files for the routers and other scripts that will need to be run on the host machine, such as the scripts to create the network tunnel to connect to the central network scenario.

The configuration assignment tool provides a link to download a zip with the configuration files. Notice that moodle does not support the distribution of a different file for each student, so in this case the personalized files need to be stored in a web server where each file has a different URL that can be assigned to each user.

The experiment is available for the students for at least two weeks. During this period, a standard moodle forum is used to give students the needed support: solving possible technical problems, answering questions about the experiment tasks, and so on.

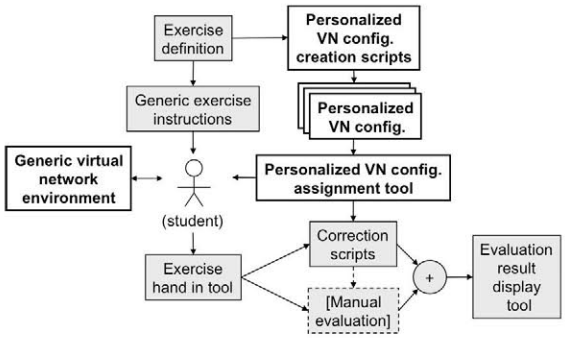

Figure 4. Personalized virtual network exercise components

Once the student completes the experiment, she can use the exercise hand in tool, which provides a form that can be configured by the teacher to allow filling in the exercise result as a set of values. A CSV file containing these values is later retrieved by the teacher. The teacher then processes the exercise results with ad-hoc scripts or spreadsheets to grade the exercise results of each student. This is combined with "manual" evaluation for those questions that do not allow a programmatically approach to evaluate the answers, for example, when questions such as "please, comment the results" are included. The result of the evaluation process will be again a CSV file including grades and feedback for each student, which will be the input for the evaluation result display tool. The student will access this tool to check her grade and the feedback provided by the teacher.

C. Student perspective

As teachers, the interest on the student perspective about these experiments is to find out how the experiments improve the teaching-learning process. In order to capture the student perspective, we will focus on two tools: a questionnaire to obtain feedback from the student, and an analysis of the evaluation results.

The questionnaire is published in the moodle server to collect feedback about personalized exercises, particularly to compare the virtual network experiments to other regular exercises that were handed-in by the students during the semester and to find out the effort needed by the students for these experiments.

In the academic year 2012/13, the OSPF/BGP routing exercise results were handed in by 105 students of a total of 127 students that handed in at least one of the personalized exercises. A total of 30 students answered the moodle questionnaire and the results were quite positive. Table I shows how students perceive this kind of exercises over virtual networks: the majority agreed that using virtual networks for all the different assignments would improve the learning of the subject.

It is also interesting to see how the students connected their network scenarios to the central backbone scenario, as shown in Table II. While more than half of the students connected remotely from their own computers, there are a significant number of students (7 out of 30) that went to the laboratory because the scenario did not boot correctly from their own computer, according to the questionnaires. At this moment, we

do not have enough information to verify the reach of this problem. In future editions of this lab experiment, we need to improve the mechanisms to collect this kind of information, for example, by including specific questions about these problems in the forms used by students to hand in their experiment results.

TABLE I. QUESTIONNAIRE RESULTS I

Doing all the assignments on virtual networks would improve the learning of the subject		
Answer	***No. of answers***	***Percentage***
1 - totally disagree	2	6.7%
2 - mostly disagree	0	0%
3 - seldom disagree	1	3.3%
4 - seldom agree	8	26.7%
5 - mostly agree	10	33.3%
6 - totally agree	9	30.0%

TABLE II. QUESTIONNAIRE RESULTS II

I ran the network scenario…		
Answer	***No. of answers***	***Percentage***
1 - At the lab, I did not try on a different computer	4	13.3%
2 - At the lab, because it did not boot correctly from a different computer	7	23.3%
3 - Partly at the lab, partly on a different computer	3	10%
4 - Not at the lab, but on a different computer	16	53.3%

Another interesting information obtained from the questionnaire was the number of hours spent doing this and other exercises. The numbers show that students employ twice as much time on this exercise compared to the other exercises, which is consistent with the grade distribution for the exercises: the weight of the OSPF/BGP routing exercise is twice the weight of the other exercises.

An analysis of the evaluation results is presented in Table III, showing for the 127 students that followed the subject, if they passed the global evaluation or not and if they passed the OSPF/BGP exercise evaluation.

TABLE III. EVALUATION RESULTS

Subject evaluation	**OSPF/BGP exercise evaluation**			**Total**
	Students passing	***Students not passing***	***No hand-in***	
Students passing	80 (63.0%)	6 (4.7%)	2 (1.6 %)	88 (69.3 %)
Students not passing	18 (14.2%)	1 (0.8%)	20 (15.7%)	39 (30.7%)

Apart from the numbers shown on the table, it is interesting to notice that from the 88 students that passed this subject, 80 had also passed the exercise evaluation (90.9 %). On the other hand, from the 39 students that did not passed the subject evaluation, 20 did not hand-in the OSPF/BGP exercise results (51.3%).

V. CONCLUSIONS

The authors are interested in how the active involvement of the students interacting with a virtualized network scenario can improve the teaching-learning process, as part of an overall goal of improving the teaching of content in networks, communication systems and services subjects. We believe that this work towards creating a virtualized Internet for computer network assignments can contribute positively to this improvement.

REFERENCES

[1] L. Bellido, D. Fernández, E. Pastor and J. Berrocal, "New strategies for learning computer networks," Global Engineering Education Conference (EDUCON), 2012 IEEE.

[2] VirtualBox. [Online]. https://www.virtualbox.org/wiki/VirtualBox Accessed 30-November-2012

[3] L. Bellido, V. Mateos, V. A. Villagrá, D. Fernández and O. Walid, "Remote Access to Computer Networking Laboratories," International Conference REV2012 - Remote Engineering & Virtual Instrumentation, Bilbao, Spain.

[4] Tinc. http://www.tinc-vpn.org/ Accessed 30-November-2012

[5] Nagios Monitoring System. http://www.nagios.org Accessed 30-November-2012

[6] BGPmon. Next generation BGP Monitor. http://bgpmon.netsec.colostate.edu/ Accessed 30-November-2012