Development of a Networking Laboratory Complex

Feliksas Kuliesius, Evaldas Ousinskis  
Physics faculty, Vilnius University  
Saulutekio 9, bld. 3, LT-10222, Vilnius, Lithuania  
feliksas.kuliesius@ff.vu.lt, evaldas.ousinskis@ff.vu.lt

ABSTRACT

This paper reviews the complex system implemented for teaching the network design and management topics, taught at Vilnius University. The special attention to sustain the practical skills is foreseen in these courses. The set of training tools, blending i) the emulators, ii) the real in-class lab and iii) the remote online laboratories, is deployed with the aim to expand advantages of interactive teaching. These tools as well as their benefits and limitations in teaching process are discussed in this paper.

KEYWORDS

Network Management, Virtual/Managed Learning Environments, Remote/Online/Virtual Laboratories, Network education

1. INTRODUCTION

Nowadays, especially when services and data storage virtualization and cloud computing plays a more and more significant role in the ICT sector, the demand of enhanced high speed network infrastructure and, consequently, of well-educated network designers and administrators is growing tremendously [1]. Additionally, network engineers must possess deeper understanding of the processes occurring in converged networks with mixed services.

It is evident, that when seeking to prepare highly qualified professionals it isn’t enough to convey solely written knowledge, i.e., theoretic background – a complex teaching environment, in which special attention to hands-on labs and case studies, must be planed.

This paper reviews the lab equipment complex used in the network design and management courses, taught at Vilnius University, Faculty of Physics and the ways to achieve the predefined goals to acquire and sustain practical skills necessary for network administrators.

In general, University studies create an excellent opportunity to get not solely strong theoretical background, but also to train hands-on experience working with modern IT equipment. On the other hand science (physics) students are very curious and adoptive to technical questions that always exist when ICT is studied, so particular attention to the technical and technological side must be scheduled when delivering the courses.

2. DISCUSSION

The main goals of the networking courses, that are partly oriented to prepare students for CCNA and CCNP professional certification exams (which are recognized as de facto standard in networking qualification grading) are to prepare creative engineers that have deep understanding of technology, infrastructure and processes, related to converged, often inhomogeneous networks, and possess teamwork skills.

As evidenced after extensive discussions with industry representatives on what they expect the needs for the future graduates, there is almost nothing to add to the verbal teaching methodology, except to change and renew the content of course, adopting it to contemporary technology trends. This is due to the well-known Cisco Networking Academy Program materials [2] and other readings (W. Odom, T. Lammle, D. Teare, K. Walace and other Study Guides [3-6]) – unrivaled textbooks which can be used as a background for corresponding courses, discussing their topics in lectures and seminars.

However, to prepare well qualified professionals, special attention to practical, hands-on lab teaching must be paid.

Three ways that can be used to solidify practical skills of students are: working with real network appliances directly, remote access to equipment...
and simulators. All of them have their own pros and cons. The simulators – Packet Tracer, GNS3, IOU etc. – can be used as self-test tools, even to partly replace lab infrastructure, since they can be available everywhere you have a computer, but, unfortunately, they have limited and reduced functionality [7,8]. Packet Tracer supports only the basic functionality of real equipment. GNS3, based on Dynamips, allows to load genuine IOS, but does not support switches. IOU, may be is the best choice from the perspective of functionality, but its usability is limited due to its proprietary license limitations. An important fact is that simulators, especially GNS3 are resource consumptive software, and it is problematic to design and test more complicated network topologies.

The real equipment and the experience of working with it overcome these limitations and is more preferable, since students can perceive all aspects of network sets: solving emerging problems, simulating (quasi)real situations, setting cabling structures and, what may be the most important – learning to work in teams.

Part of the equipment of the described laboratory is available directly, part – via remote access. Direct access is very useful for beginners: students become acquainted with the appliances, they can do the cabling, see deployed topology evidently, console directly to the gear and coordinate team-work as well as consult classmates or be consulted by the instructor. The main weakness of this approach is the limited access to the equipment – we have only 10 workplaces available in our lab for such direct access training.

The way to utilize the resources and possibilities of the facility is to enable remote access, which can be solved in different ways [9-11]. Additionally, remote access helps to develop creativity, mental visual thinking and the imagination, which is necessary striving to better perceive the maintained infrastructure. In other words, remote access manner accustoms the students to the conditions close to real ones which the administrators face every day when monitoring and configuring extended networks.

When designing the lab, the main points that were pursued were: in order to meet the needs of students to experiment effectively, handily and securely, the main labs (CCNP, Security and Service provider lab racks) were devoted for common collaborative use. They can be accessed via a different VPN connection per each lab pod. The conventional Cisco Easy VPN implemented on Cisco ASA 5510 Firewall was used to safeguard the authenticated and secured connection to the each of pod access server. Pre-shared keys for individuals or all users of the group, intended to access the pods, were used. So, a single pod (or some of them, connected in a bigger cluster) can be used personally or by a team, depending on the teaching goals. The appliances can be consoled in using reverse lines of access server (Cisco 2511 or 1841 routers with HWIC-8A cards). To visualize the lab topology, the access server menu was mapped and hyperlinked to the topology diagram on the web server, attached to the pod. So, selecting a device icon, the user should be connected into the appropriate device console. The versatile CCNP lab topology, adopted both to our own customized labs, and to the standard labs from Student Lab Guide [12], designed to meet all three required courses (ROUTE, SWITCH, TSHOOT) is presented in Fig.1. The PCs and servers, required for testing, authenticating and monitoring lab equipment were installed as virtual machines (VM) using VMware ESXi 5.0 hypervisor on the Dell PowerEdge R210 server. One of the each PC interfaces was configured in a different VLAN denoted for this PC on VMware virtual switches, trunked to Catalyst 2960 switch (not shown in diagram) and separated by it. Additional VM can easily be deployed under request. FTP, TFTP, DHCP, RADIUS, TACACS, Syslog servers and network monitoring tools like Wireshark, Zenoss [13] and others were implemented as test instruments into these VM machines. Some security restrictions are applied to prevent machine misusing, e.g., misconfiguration of management connections.

To access the PCs’ remote desktop more conveniently than using the usual RDP, TinyVNC was installed into each PC/Server of the lab, and these PCs became reachable via web browser, without a need of RDP client.

The electric supply of the devices was controlled by Internet driven APC switched rack PDUs, model AP7953, which enabled the user to switch the lab equipment on/off when needed remotely. On the start or full reload of the
laboratory pod, each device should be started with an appropriate delay to prevent power overload. These labs fully solved the access problem, since students can access the labs 24x7 from anywhere. It is convenient to organize the teamwork training using group login in such a way. From the point of the instructor, the only downside of the system is that it is difficult to track and evaluate student performance, since the instructor often sees only the final result, without intermediate actions. So, it is difficult to help the students timely, if needed. The opportunity to evaluate student’s operation sequence is essential when organizing hands-on skills exam. To utilize the resources and possibilities of the facility to achieve the before mentioned goals, the lab system was supplemented with the lab management system which ensures i) individualized access to the lab with time reservation, ii) database of predefined lab tasks, iii) tracking the student actions and iv) securing the system from misusing.

This additional management system has been deployed into some pods of the lab cluster. The structural model of the managed lab is presented in Fig. 2. The management system consists of i) the server, dedicated for the main control of processes such as a RADIUS server, a MySQL database, and an Apache HTTP server as a platform for the web user and administrator/instructor interfaces adapted for the user registration, the lab time reservation, the control of lab devices and power supply, the monitoring of students’ activities as well as for the storage of lab descriptions, assignments and other materials; ii) the intrusion prevention system (based on Suricata [14]) designed for monitoring and securing the system. The main server of the lab on the basis of Ubuntu 11.10 installed upon the same VMware ESXi 5.0 hypervisor where the lab PCs reside, has been used. The desired functionality is achieved by installing a FreeRadius – tiny, modular and flexible server which includes not only AAA services, but usual LAMP and additional ones [15]. When designing and deploying laboratory web interface the PHP, HTTP, CSS, Java Script with jQuery framework library were used. The
control of the devices was realized using AJAX and Java Web Start technologies.

With the aim to heighten the security level of the virtual machines, additional scripts were implemented into management server. The user was not only restricted to the rights and commands which are necessary to solve the assignments presented only, but, due to these scripts the possibility to easily recover the PC appeared. After the misconfiguration or other unpredicted change it is enough to restart the VM which is configured so that after its reboot the configuration and storages are restored to the initial state. Reboot is available not only from the VM desktop (impossible after system hang-up), but from the system management panel also (the same way the power supply and network devices (routes, switches etc.) reset or the pre-configuration load (described below) can be initiated).

It is more difficult to control unwanted actions of the users connected into the network equipment. These tasks were resolved when using Suricata IPS, through which all user traffic was directed. IPS filtered unwanted commands and generated logs for user activity monitoring.

To secure the user reservation, a RADIUS server and access to real lab equipment time synchronization, the cron processes were used. To use this system, students must register and fill-in a lab user profile with a nickname, password, real name and email address. The registration must be approved by the lab administrator in order to reject illegal users.

When the user chooses the reservation time in the calendar the temporal password valid for the reservation time only is generated and sent to the user. The access server allows connections to the lab appliances only for the user, which successfully passes the RADIUS authentication. Connecting to the lab on the reserved time the student can start the desired assignment. To feel more convenient and to save time, the assignments are supplied with preconfigured devices. This also allows the instructor to design specific tasks, especially necessary in the troubleshooting course. Each lab assignment is described by a separate URL element which generates an appropriate assignment description view and loads the predefined configurations onto the lab appliances:

```html
<ul class="lab">
  <li>Lab 1-1: Switching basics</li>
  <li><a href="Labs/SW_Lab_1_1" data-link="http://172.16.83.53/ConfigurationLoad/LoadLab/Switch/lab_1_1" class="start">Begin</a></li>
  <li><a href="/assets/pdfs/Switch/Lab_1_1.pdf" title="Switch Lab 1-1 Description" alt="Switch Lab 1-1 Description" target="_blank" class="description">Assignment description</a></li>
</ul>
```

Since it is impossible to use two hyperlinks (HREF attributes executed in range) directly the additional attribute data-link="http://172.16.83.53/ConfigurationLoad/LoadLab/Switch/lab_1_1" is used to load the predefined configurations. The loading of the configuration is activated by this javascript code:

```javascript
$(function(){
  var seconds = 1;
  var canClick = true;
  seconds *= 1000;

  /* HIDE DESCRIPTION. (Hide "Description"
equipment and iii) remote labs – each of them having different benefits – it has been succeeded to prepare highly qualified network administrators and designers, feeling confident in challenging labor situations. The management system enables the instructor to track a student’s intermediate actions, to correct and advise him/her if required as well as evaluate their activity more accurately.

The special components of the management system allow the user – the student and the instructor as well – to feel handily with the lab assignments and to focus on solving the main tasks.

4. REFERENCES