Virtual Laboratory for Cisco Networking Academy Program

Delyan Genkov

Abstract: *The Cisco Networking Academy Program is established in 1997 and become very popular today. Now there are more than 10,000 academies in 165 countries and more than 1,000,000 students worldwide. Teaching in the program includes online lectures, exams and laboratory exercises on real equipment and/or simulators. Present paper proposes a way to create a virtual laboratory, which provides distant access to real equipment without risk of losing access due to misconfiguration of devices.*
Key words: *Distance learning, Virtual Laboratory, Cisco Networking Academy, Remote access.*

INTRODUCTION

The Cisco Networking Academy Program is established in 1997 and become very popular today. Now there are more than 10,000 academies in 165 countries and more than 1,000,000 students worldwide [1].

Technical University of Gabrovo maintains the first Cisco Networking Academy in Bulgaria since 1999. Our education in this program is apart from the regular student's education and is taught as complementary courses.

Some of our students have difficulties to be present in class, because they live in different parts of the country and some of them are working in parallel with studying. For some students learning in working hours is not possible and they prefer to learn on holidays or after work hours. That's why we tried to create some form of distance learning for them. There is not a problem with the lectures and exam tests, because the students can access the necessary materials online through the Cisco's Netspace platform, but we had difficulties with laboratory exercises, where an access to real equipment is needed. Although some simulation platforms exist, like Cisco Packet Tracer, they do not support all the necessary options and sometimes differ from the real situation. It is definitely better when the students work on real equipment.

Cisco devices have several options for configuration. The first and only possible option without initial configuration is through their console port – a serial port, which must be connected to a computer with terminal software. This option is always available and at least the device can be reset without configuration in every circumstance, but it requires direct connection to the device. Other configuration options include remote access through telnet, SSH, HTTP, etc., but all of them require some initial configuration – at least IP address information and passwords for access. It is possible when someone is connected to a device remotely to change configuration (e.g. the IP address) and thus to lose the access to the device. In this case the device must be accessed through the console and the configuration to be corrected for remote access.

Sometimes our laboratory exercises starts without configurations, but sometimes the devices must have some initial configurations. Because the cabling connections can't be done remotely, we revised all the laboratory setups to have a single physical topology, and it is connected in advance.

RELATED WORK

Some companies like NIL and Comstor provides paid access to real equipment, but they don't publish any technical details about realization of their virtual laboratories. One possible solution is described by Dan Alberghetti in [1], but it requires a separate computer, connected to every router or switch and remote access is established through a VPN connection and remote desktop. In his work [6] Orlin Tomov describes an approach for establishing a remote access to real equipment, but the devices used are single-chip microcontrollers and the specific Cisco issues like reset of configurations and/or passwords are not addressed. Valchanov and Yuseinov propose a virtual Cisco laboratory in [7], but here are provided access to simulated, instead of real devices.

VIRTUAL LABORATORY STRUCTURE

As mentioned above it is essential to provide access to the console port to remote users. Another issue is to provide the possibility for some standard initial configurations of the devices as well as resetting the devices in case of wrong configuration.

Our equipment rack consists of eight devices – four routers Cisco 2821 and four switches – two Cisco 2960 and two Cisco 3560. For the needs of the virtual laboratory we need to manage power connections for reset and serial connections for configuration of these eight devices. That's why we established the structure of the laboratory as shown on Figure 1.
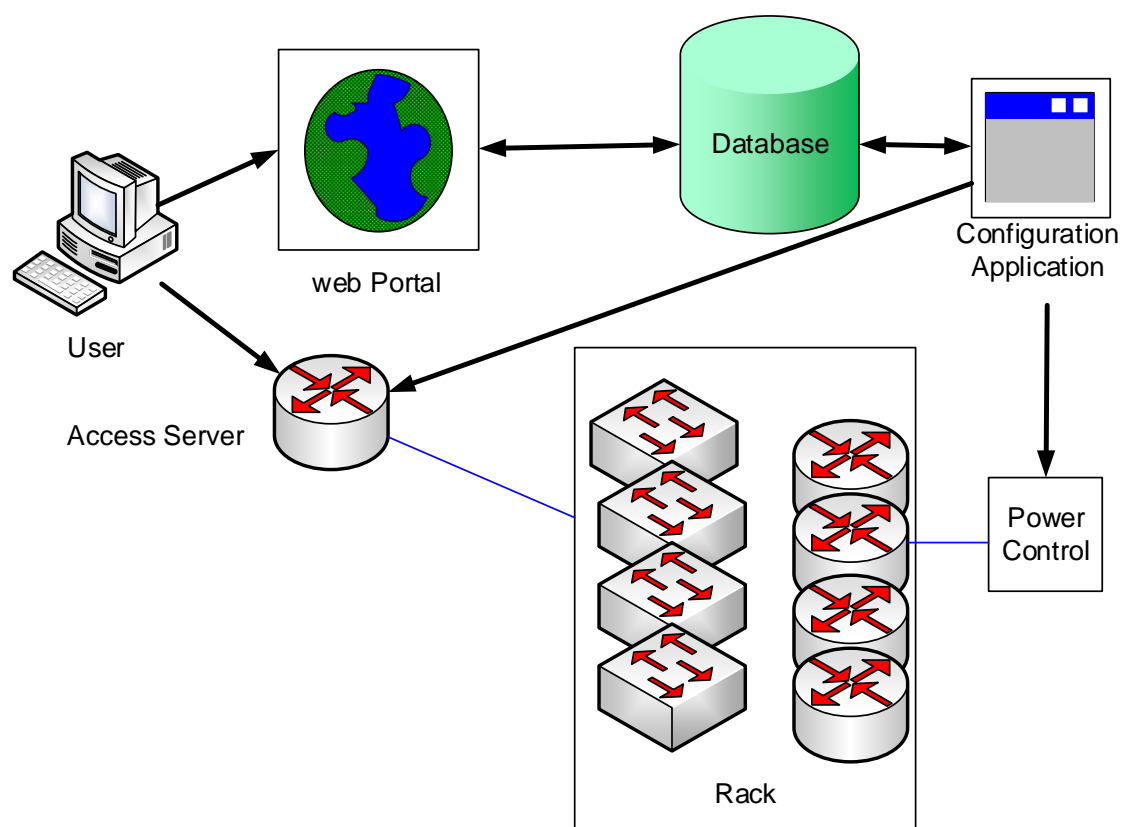

Figure 1. Virtual Laboratory Structure

The user must have registered username and password and through the web portal he can reserve date and time for remote access to the rack. Now the time slots are at one hour intervals and there is no restriction how many slots an user may reserve, but it is possible to restrict this. Along with reservation the user can select an initial configuration to be done on the devices from a set of predefined configurations. These reservations are written in the database and in five minutes before the reservation time the configuration application resets the devices, clears their configurations and installs the requested configuration files if any. Then the user can access the devices console ports through a telnet (SSH) session to the access server.

The access server is a Cisco 2511 router, which has 16 asynchronous serial ports [3]. In this setup we are using only the first eight, connected with an octal cable to the console ports of the eight devices. Its console port is connected to the computer where the configuration application is running and its Ethernet port is connected to the network with a public IP address and telnet and SSH sessions are enabled. The remote user logins into the access server and the only options are to make a reverse telnet connections to console ports of the rack devices. The reverse telnet session must be done on port number 2000 + the number of the device, for example the first router is available like this:

```
AccessServer#telnet 192.168.1.1 2001
Trying 192.168.1.1 ...
Router1#
```

A remote user can make up to five simultaneous telnet or SSH sessions to the access server and then remote telnet sessions with five different devices or to make many reverse telnet sessions from a single remote session and to switch between them, pressing the session number (e.g. 1).

In case of misconfiguration of a device, the user may request a device reset from the web portal. The reset procedure is described later.

The configuration application is responsible for initial setup of the devices and for reset of some device upon a user request. Five minutes before a reservation time the configuration application disconnects remote sessions with the access server if any, resets all the devices and installs the initial configurations of the devices, if this is requested by the user.

The reset procedure is slightly different for routers and switches, but it requires switching off and on the power of the devices. In the first 30 seconds of the boot time the software sends a break signal to the device thus interrupts the device's boot process and enters in ROMMON mode. This is necessary because the user may have changed the passwords for access to the device. After breaking the boot process the configuration register is changed, instructing device to boot without configuration and without password for access through console port [4]. Then the device is booted manually, the existing configuration is deleted, and a new configuration is uploaded if requested by user. Last the configuration register is restored to the original value and the device is rebooted again. The whole process takes about 4 minutes on Cisco 2811 router. The reset process is similar for switches, but from ROMMON mode two files are deleted and device is booted without configuration in only one restart. If the password for the switch is unknown, the reset procedure requires manual pressing of the "Mode" button during restart.

For power management of the devices an USB relay board is used. It is shown at Figure 2.
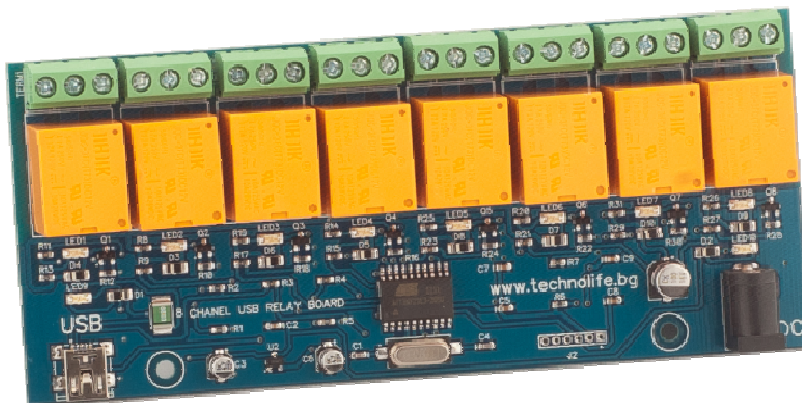

Figure 2. Relay Power Management Board

The relay control is built into the configuration application through an SDK, which comes with the board. Power connections of all the eight devices passes through the relays and the application power cycles the devices when needed.

The web portal is written in PHP and HTML 5 and an example screen is shown at Figure 3.
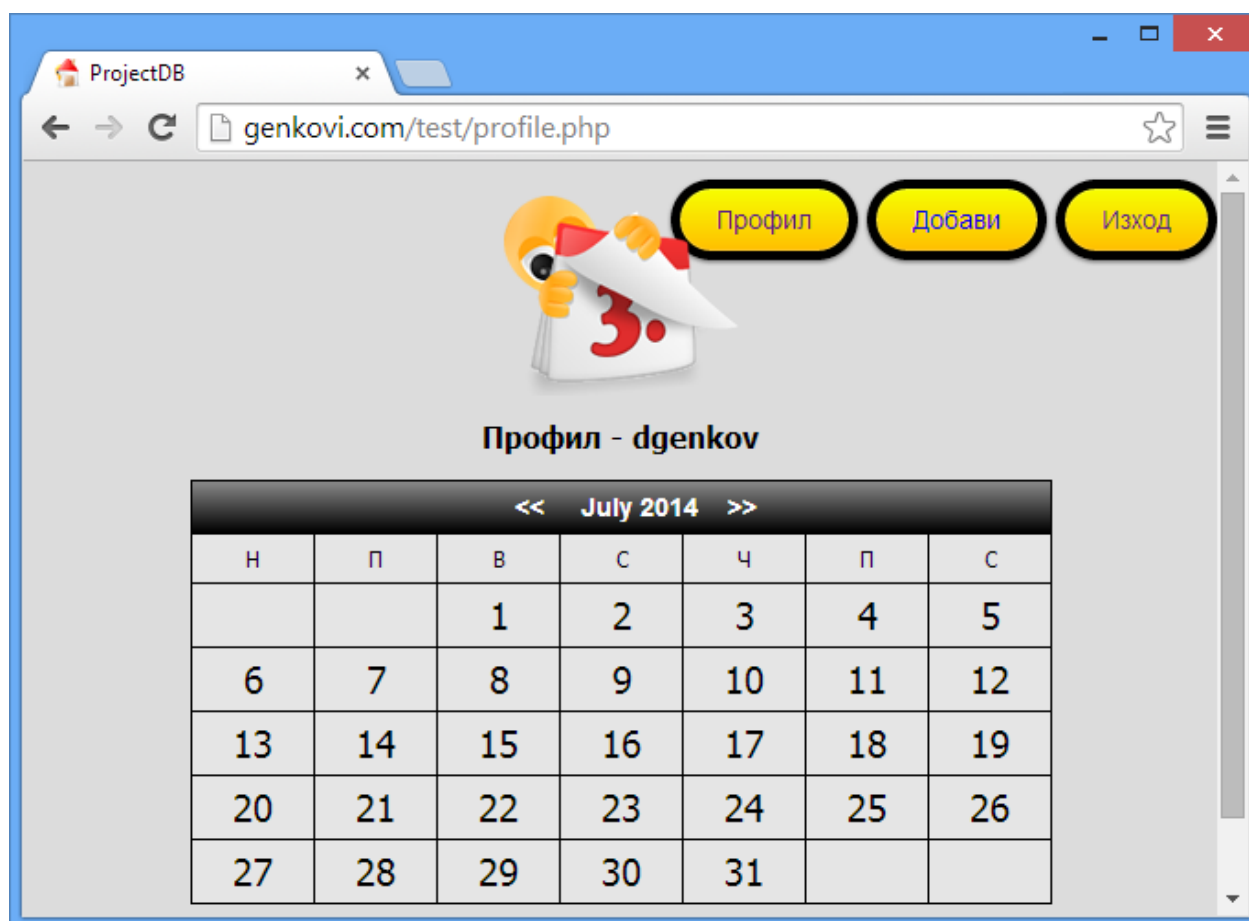
Figure 3. Web portal

The database used is MySQL. The configuration application is written in C# using Microsoft Visual Studio 2010, and a sample screen from it is shown at Figure 4.

Through this application an administrator can manually reset some or all of the devices, optionally selecting a configuration that have to be uploaded to any device. A device may be marked as inactive, which means that the commands from the software will not be applied to this device. Because of different reset procedures, the device type – router or switch must be selected. The reset procedure is performed automatically five minutes before the allocated time slot. Manual reset from the user is performed through a web interface – when the user requires reset of some device, he can press the corresponding button on the web interface, then this request is written to the database, and last it is performed by the configuration application.
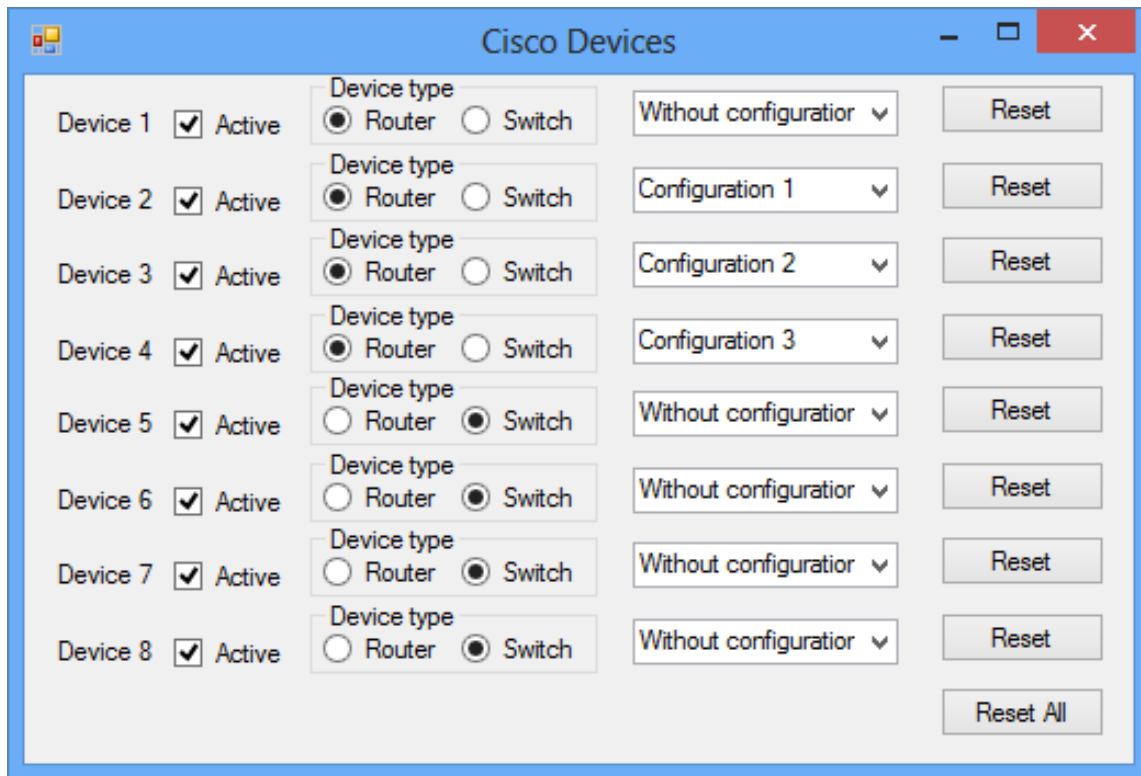
Figure 4. Configuration application

RESULTS

Now our virtual laboratory is in testing period, but there is a great interest from our students. Sometimes they reserve night sessions, which is another benefit – the laboratory is accessible 24 hours per day and can be used from people residing in different time zones.

At this time we can provide only one student's access at a time, because we have only one rack, but this setup can be multiplied. Actually the access server can handle five simultaneous telnet connections, so with one access server we can handle remote access for five users through this virtual lab, but at this time we haven't enough equipment for remote access.

Current implementation can be used for eight devices, but the access server has 16 asynchronous ports and with another relay board and small software changes it can be used for up to 16 devices. If more devices are needed an additional access server with different public IP address can be added.

CONCLUSIONS AND FUTURE WORK

Present paper proposes a way to organize a virtual laboratory with Cisco devices. It can be used to provide remote access to real equipment without the need of initial configurations of the devices. This approach also protects users from losing connection to the devices due to misconfiguration, which is a common issue with not very skilled students. It also provides a way for recovering unknown passwords, set to devices by other users.

Some future enhancements are planned, including improved user control, accounting of the commands issued from the user and the possibility for automation of assessment of the results from configuration.

ACKNOWLEDGEMENTS

REFERENCES

[1] Alberghetti, Dan, Remotely Connect to a CCNA Lab Topology, http://www.danscourses.com/CCNA-1/remotely-connect-to-a-ccna-lab-topology.html, date of usage 19.08.2014.

[2] Cisco Systems. The Cisco Networking Academy Program. https://www.netacad.com/web/about-us/about-networking-academy, date of usage 12.07.2014.

[3] Cisco Systems. Cisco 2500 Series Router Architecture. http://www.cisco.com/c/en/us/support/docs/routers/2500-series-routers/5750-arch-2500-5750.html, date of usage 12.07.2014.

[4] Cisco Systems. Password Recovery Procedure for the Cisco 2600 and 2800 Series Routers. http://www.cisco.com/c/en/us/support/docs/routers/2600-series-multiservice-platforms/22188-pswdrec-2600.html, date of usage 12.07.2014.

[5] Cisco Systems. Use of the Configuration Register on All Cisco Routers. http://www.cisco.com/c/en/us/support/docs/routers/10000-series-routers/50421-config-register-use.html, date of usage 12.07.2014.

[6] Tomov, Orlin, Virtual labs with remote access to a real hardware equipment in the computer systems education, In proceedings of International Conference on Computer Systems and Technologies - CompSysTech'08, Gabrovo, pp V.17-1 - V.17-5

[7] Valchanov, Hristo, I. Yuseinov, A Virtualized Networking Laboratory, in proceedings of UNITECH 2012, Gabrovo, pp I473-I477

ABOUT THE AUTHOR

Principal Assistant Prof. Delyan Genkov, PhD, Department of Computer Systems and Technologies, Technical University of Gabrovo, Phone: +359 66 827 501, E-mail: dgenkov@tugab.bg.

The paper has been reviewed.